

PÓNTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR



FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN REDES DE COMUNICACIONES

TEMA:

**PROPUESTA MÉTODO DE MIGRACIÓN Y COEXISTENCIA DE IPV6
SOBRE RED IP/MPLS PARA ENTREGA DE SERVICIOS DE
CONECTIVIDAD A CLIENTES CORPORATIVOS DE CNT EP.**

PALACIOS SAMPEDRO LUIS GUSTAVO

Quito – 2016

AUTORÍA

Yo, Luis Gustavo Palacios Sampedro portador de la cédula de ciudadanía No 0103426045, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

Luis Gustavo Palacios Sampedro

N

Contenido

1. INTRODUCCIÓN.....	1
2. JUSTIFICACIÓN	3
3. ANTECEDENTES	4
4. OBJETIVOS.....	6
Objetivo General:	6
Objetivos Específicos:.....	6
5. DESARROLLO CASO DE ESTUDIO	7
5.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED IP/MPLS DE CNT EP	7
5.1.2 Red IP/MPLS	7
5.1.3 Modelo Jerárquico	9
Capa de núcleo o de Core.....	9
Capa Distribución.....	10
Capa de Acceso	11
Nomenclatura de los equipos MPLS	12
5.1.3 Configuración de los equipos de la red IP/MPLS de CNT EP	12
Protocolo de Internet IPv4 en el Red MPLS	12
Interfaz loopback.....	13
IP CEF.....	13
Protocolo de Distribución de Etiquetas LDP	14
Protocolo de enrutamiento interno IS-IS (Intermediate system to intermediate system)	14
Protocolo de Puerta de Enlace de Borde (BGP)	15
Calidad de Servicio QoS	16
5.1.4 Configuración de Clientes Corporativos en la Red IP/MPLS de CNT EP	18
Configuración de la VRF	18
Configuración Red Privada Virtual (VPN) en MPLS	19
Configuración de Direccionamiento IP en la Interfaz.....	19

5.1.5 Resumen de la situación actual de Red IP/MPLS CNT EP	20
5.2 MÉTODOS DE MIGRACIÓN & COEXISTENCIA DE IPV4 E IPV6.....	22
5.2.1 Métodos de migración y coexistencia de IPv4 / IPv6 sobre red IP/MPLS	23
5.2.1.1 IPv6 sobre circuitos de transporte MPLS.....	23
5.2.1.2 IPv6 con túneles en los routers CE	24
5.2.1.3 Provider Edge 6PE - IPv6 sobre MPLS en los equipos de borde del proveedor PE.....	25
5.2.1.4 Método 6VPE - IPv6 VPN sobre MPLS en los equipos de borde del proveedor PE.....	26
5.2.2 Resumen de métodos de migración.	27
5.3 PROPUESTA DEL MÉTODO DE MIGRACIÓN Y COEXISTENCIA IPV4 & IPV6 SOBRE RED IP/MPLS DE CNT EP	29
5.3.1 Análisis de requerimientos de Hardware y Software para la migración / coexistencia.....	30
5.3.2 Análisis de tráfico en la red IP/MPLS con IPv6	32
5.4 SIMULACIÓN SITUACIÓN ACTUAL DE LA RED IP/MPLS.	37
5.5 SIMULACIÓN DE RED IP/MPLS IMPLEMENTADO IPV6 CON EL MÉTODO 6VPE.....	42
Diagrama red IP/MPLS con el Método 6VPE para habilitar IPv6.....	42
Habilitación del protocolo de internet IPv6	43
Configuración Instancia de enrutamiento VRF para cliente	43
Configuración dirección IPv6 en la interfaz	44
Configuración Red Privada Virtual (VPNv6) en MPLS	45
5.5.1 Configuración IPv6 en el equipo el cliente CE.....	46
5.5.2 Comparación de configuración de IPv4/ IPv6 sobre red IP/MPLS utilizando el método 6VPE.	47
5.5.3 Resultados al implementar 6VPE en la red IP/MPLS.....	49
Verificar VPNv6-MPLS en los equipos de borde donde la VRF tenga presencia.	49
Coexistencia de Protocolo IPv4 e IPv6 en los equipos de borde PE.....	49
Conectividad desde los equipos de Borde PE a la Instancia de Enrutamientos VRF de los clientes.....	50

Verificación que los equipos de Core mantienen direccionamiento IPv4	51
5.6 ANÁLISIS DE LA MIGRACIÓN & COEXISTENCIA DE IPV4 E IPV6 PARA CLIENTES CORPORATIVOS EN LA RED IP/MPLS DE CNT EP	53
6. CONCLUSIONES Y RECOMENDACIONES	54
6.1 Conclusiones	54
6.2 Recomendaciones.....	55
7. BIBLIOGRAFIA.....	56

INDICE DE FIGURAS

Figura 1. Componentes y operación de la red MPLS [11].....	8
Figura 2. Nivel Jerárquico de CNT EP. [Elaborado por el autor]	9
Figura 3. Interfaz loopback en equipos de Red IP/MPLS. [19]	13
Figura 4. CEF habilitado en la Red MPLS CNT EP. [19]	14
Figura 5. LDP habilitado en la Red MPLS CNT EP. [19]	14
Figura 6. Configuración IS-IS en red MPLS de CNT. [19]	15
Figura 7. Proceso 28006 de BGP de CNT EP. [19]	16
Figura 8. Class-Map de CNT EP. [Elaborado por el autor]	16
Figura 9. Class-Map en equipo de Distribución de Mariscal [19]	17
Figura 10. Configuración Class-Map en equipo de Distribución de Mariscal. [19]	17
Figura 11. Configuración de VRF de un cliente. [19]	18
Figura 12. Address family en BGP 28006. [19]	19
Figura 13. Configuración de interfaz VLAN asociado a VRF. [19]	20
Figura 14. IPv6 sobre circuitos de transporte sobre MPLS [12]	24
Figura 15. IPv6 con túneles en los routers CE [5]	25
Figura 16. Topología de método 6PE [8]	26
Figura 17. Funcionamiento método 6VPE [5]	27
Figura 18. Comando show versión para obtener información del equipo. [19]	30
Figura 19. Número de Equipos de Distribución por serie. [Elaborado por el autor]	31
Figura 20. Trafico en interfaz de Equipo PE – P. [Elaborado por el autor]	33
Figura 21. Trafico del equipo UIOQCNP01 – UIOMCHE01. [18]	33
Figura 22. Isla Trinitaria Pe – Guayaquil P. [18]	34
Figura 23. Guayaquil Kennedy PE – Guayaquil P. [18]	35
Figura 24. Cuenca Gualaceo PE – Cuenca P. [18]	35
Figura 25. Estación Terrena PE – Quito Centro P. [18]	35
Figura 26. Ibarra Centro PE – Ibarra P. [18]	35
Figura 27. Esquema simulado de la Situación Actual de la Red IP/MPLS. [17]	38
Figura 28. Verificación de funcionamiento Protocolo MPLS. [17]	39
Figura 29. Verificación de funcionamiento Protocolo ISIS. [17]	39
Figura 30. Verificación de funcionamiento Protocolo BGP. [17]	39
Figura 31. Prueba de conectividad desde UIOMSCE01 a AMBCNTE01. [17]	40
Figura 32. Pruebas de conectividad de clientes. [17]	41
Figura 33. Esquema y direccionamiento IP para simulación del método 6VPE. [17]	43
Figura 34. Configuración de VRF definition. [17]	44

Figura 35. Configuración interfaz con IPv6. [17].....	45
Figura 36. Configuración VPNv6. [17].....	45
Figura 37. Configuración address-family IPv6. [17].....	46
Figura 38. Configuración IP_WAN cliente. [17]	46
Figura 39. Verificación del Tunel VPNv6 –MPLS cliente 1. [17].....	49
Figura 40. Pruebas de conectividad IPv4 e IPv6 del cliente utilizando VRF. [17]	50
Figura 41. Pruebas de conectividad desde MPLS hacia la WAN. [17].....	51
Figura 42. Pruebas de conectividad equipos CE de Matriz y Sucursal del Cliente_1. [17] ..	51
Figura 43. Prueba tracer desde CPE_Matriz hacia CPE_sucursal. [17].....	52

INDICE DE TABLAS.

Tabla 1. Equipos de Core de CNT EP. [Elaborado por el autor]	10
Tabla 2. Equipos de distribución de CNT EP. [Elaborado por el autor]	11
Tabla 3. Ejemplo de nomenclatura de los equipos MPLS. [Elaborado por el autor]	12
Tabla 4. Class-Map de CNT EP. [Elaborado por el autor]	16
Tabla 5. Resumen de la situación actual de RED/IP MPLS de CNT EP. [Elaborado por el autor]	21
Tabla 6. Resumen de métodos de IPv6 sobre MPLS. [Elaborado por el autor]	28
Tabla 7. Características de métodos de migración en base a la situación actual de la Red. [Elaborado por el autor]	29
Tabla 8. Equipos PE de CNT EP Hardware y software. [Elaborado por el autor]	31
Tabla 9. Características de los equipos PE de CNT. [Elaborado por el autor]	32
Tabla 10. Análisis de Trafico con IPv6 entre equipos PE-P. [Elaborado por el autor]	36
Tabla 11. Direccionamiento IP Simulación Actual de Red. [Elaborado por el autor]	37
Tabla 12. Direccionamiento IP Para activar IS-IS. [Elaborado por el autor]	37
Tabla 13. Direccionamiento IP para Cliente corporativo. [Elaborado por el autor]	40
Tabla 14. Direccionamiento IPv6 utilizado para simulación. [Elaborado por el autor]	44
Tabla 15. Direccionamiento IPv6 configurado en el cliente. [Elaborado por el autor]	46
Tabla 16. Comparación de Configuración IPv4 y el método 6VPE. [Elaborado por el autor]	48

1. INTRODUCCIÓN

El uso del internet ha tenido un crecimiento exponencial, principalmente desde que se le dio un uso comercial, por lo que los dispositivos necesitan de direcciones IP para conectarse a la red. EL Protocolo IPv4 se ha venido utilizando aproximadamente más de treinta años y al tener un espacio de 32 bits para expresar esta dirección se tendría alrededor de 4.300 millones de IPs, pero esta cifra se reduce considerablemente al tener direcciones reservadas, privadas, no utilizables, malos asignamientos entre otros. La nueva versión del protocolo de Internet IPv6 ha mejorado en varios aspectos a su antecesor, siendo la principal ventaja el mayor espacio de direcciones, teniendo una longitud de 128 bits, aproximadamente 340 sextillones de direcciones IP, es decir se puede tener cerca 4300 millones de IPs por metro cuadrado. Con estas referencias y frente al agotamiento de direcciones IPv4 a nivel global, varias empresas a alrededor del mundo han empezado a trabajar en un método de transición hacia el nuevo protocolo de internet IPv6.

En Junio del 2014 la LACNIC anuncio haber alcanzado la cota de 4.194.302 IPv4 (/10) en su stock, complementariamente el Gobierno Nacional del Ecuador dentro del Plan Nacional de Desarrollo de la Banda Ancha cita la transición y coexistencia de IPv4 & IPv6, por lo que la Corporación Nacional de Telecomunicaciones CNT EP se ha visto en la obligación de realizar varios análisis de sus diferentes plataformas (Backbone IP/MPLS, Servidores, Equipos de virtualización , Equipos de Transmisión, sistemas de Gestion/Monitoreo etc,) para poder efectuar la coexistencia y migración a IPv4 & IPv6.

En el presente caso de estudio se realiza una propuesta de método de migración / coexistencia para diseño de una red IPv6 sobre backbone IP/MPLS dirigido al segmento Corporativo de CNT EP, donde se citará y estudiará varios conceptos relevantes a la tecnología como protocolo IP/MPLS, métodos de transición / coexistencia, complementariamente se realiza el análisis de la situación actual de Red MPLS referente a

configuración lógica, tráfico, Hardware y Software etc para poder determinar el mejor método de migración a IPv6 que mejor se ajuste a las necesidades de la empresa. Con la finalidad de minimizar los errores de configuración en la plataforma activa de la red se realizara una simulación de la situación actual de la Red y los cambios en la configuración para poder entregar el servicio de conectividad con IPv6 a clientes corporativos. El objetivo final es tener una metodología para la inicialización de pruebas con IPv6 en enlaces (datos e internet) del segmento corporativo.

2. JUSTIFICACIÓN

El área de Solución Técnica Corporativa de CNT EP entre sus funciones se encuentra realizar el levantamiento técnico, instalación y configuración de los enlaces corporativos, por lo que tiene la responsabilidad de iniciar con el proceso de coexistencia y transición IPv4 e IPv6 en los enlaces de conectividad fijos (Datos e Internet) dirigido al segmento corporativo.

En el presente caso de estudio se realizara una propuesta de un método de migración / coexistencia para diseño de una red IPv6 sobre backbone IP/MPLS dirigido al segmento Corporativo de CNT EP, donde detallara los métodos de transición & coexistencia hacia IPv6 que mejor se ajusten a las necesidades de la empresa. Se analizará la situación actual de la red referente a: equipos que forman la red IP/MPLS, software, protocolos de conectividad que se encuentran habilitados, con el objetivo de poder determinar la mejor técnica de migración y coexistencia de IPv6. Complementariamente se examinará los diferentes cambios que el backbone IP/MPLS tendrá luego de establecer el método de migración, se revisará el cambio lógico a realizarse en la configuración de la red, se analizará el aumento de del ancho de banda que se tendrá al utilizar IPv6.

Con la finalidad de reforzar el análisis y verificar que la propuesta establecida se la que mejor se ajuste a las necesidades de CNT EP se realizara una simulación de la red IP/MPLS con los cambios establecidos para el nuevo protocolo IPv6, para validar su funcionamiento en cuanto a conectividad, de esta manera minimizar los errores de configuración que se puedan producir al modelar directamente en la plataforma activa de CNT EP.

3. ANTECEDENTES

Con el crecimiento exponencial en la tecnología y el uso masivo del internet a nivel mundial, se acerca el agotamiento de IPv4 el mismo que se viene utilizando aproximadamente desde 1981. La siguiente evolución del Protocolo de internet es IPv6 que se terminó de desarrollar en 1996 incorporando varias mejoras y sobre todo la característica principal un espacio de direccionamiento muy grande es decir se podrá tener 4300 millones direcciones IPv6 por metro cuadrado disponibles para todo el planeta Tierra.

A mediados de Junio del 2014 la LACNIC (Registros de Direcciones de Internet para Latinoamérica y el Caribe) anuncio haber alcanzado la cota de 4.194.302 IPv4 (/10) en su stock, que en la práctica significa el agotamiento de las direcciones IPv4 por lo que empieza a regir políticas restrictivas para la entrega de recursos de internet. Durante esta fase de agotamiento de IPv4 la LACNIC podrá asignar 2.097.150 de las 4.194.302 direcciones remanentes, en bloques limitados de entre 256 (/24) y 1.024 (/22), las organizaciones solamente podrán solicitar un bloque adicional luego de seis meses de haber recibido su última asignación. Cuando se agoten cerca de las 2 millones de IPs indicadas, los miembros de LACNIC ya no podrán recibir más asignaciones de recursos IPv4. El IANA asignado un pool /12 de IPv6 a la LANIC para que puede ser distribuido a sus cliente.

Por otro lado uno de los proyectos más ambiciosos del Gobierno Ecuatoriano es llevar al país hacia el mundo de la nueva era digital, en el Plan Nacional de Desarrollo de la Banda Ancha, que fue elaborado y presentado por el Ministerio de Telecomunicaciones y Sociedad de la Información, dentro del marco **Estrategia de Ecuador Digital 2.0** se cita la transición y coexistencia de IPV4 & IPV6.

Con los antecedentes citados la Corporación Nacional de Telecomunicaciones CNT EP y al ser miembro de LACNIC se acoge a las políticas restrictivas de asignación de IPv4 debido al agotamiento existente. Complementariamente viene apoyando en el proyecto de gobierno citado anteriormente por lo que esta empresa está realizando varios análisis para la entrega

del servicio de conectividad mediante el nuevo protocolo de Internet IPv6 mejorando la calidad de servicio, pudiendo de esta manera brindar mayor espacio de direcciones IP a cada cliente.

4. OBJETIVOS

Objetivo General:

Propuesta método de migración y coexistencia de IPv6 sobre red IP/MPLS para entrega de servicios de conectividad a clientes corporativos de CNT EP.

Objetivos Específicos:

1. Analizar la situación actual de red IP/MPLS de CNT EP
2. Detallar los diferentes métodos para la migración / coexistencia de IPv4 & IPv6 sobre IP/MPLS.
3. Establecer una propuesta y método de migración y coexistencia de IPv4 & IPv6 sobre red IP/MPLS.
4. Simular la configuración actual de la red IP/MPLS con servicios de conectividad de clientes corporativos.
5. Simular la configuración del protocolo IPv6 en la red IP/MPLS con servicios de conectividad de clientes corporativos.

5. DESARROLLO CASO DE ESTUDIO

5.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED IP/MPLS DE CNT EP

La Corporación Nacional de Telecomunicaciones CNT EP es una empresa de telecomunicaciones que cuenta con una red IP/MPLS, tiene un backbone en topología anillo contando aproximadamente con más 12Km de FO con redundancia a nivel de Core y distribución, aproximadamente 2400 equipos que forman la red MPLS.

Las principales características de Red IP/MPLS de CNT EP se citan en la presente sección, para poder determinar: hardware, software, protocolos de enrutamiento, configuración lógica, direccionamiento IP, que intervienen actualmente en el funcionamiento de la red para brindar conectividad. Esto servirá de base para analizar el método de migración que se ajustará a la necesidad de CNT EP.

5.1.2 Red IP/MPLS

La red de CNT EP utiliza el protocolo MPLS (Multi-Protocol Label Switching) que es una tecnología envío de paquetes utilizando etiquetas de tamaño fijo para tomar la decisión de envío de datos. Las etiquetas usualmente corresponden a las redes de destino IP (similar a IP tradicional) pero combinando las mejores funciones de la capa 3 (ruteo) y las de capa 2 (switching).

Elementos de Red MPLS

Para entender generalmente el concepto de MPLS sobre el cual funciona la red de CNT EP, se detalla los elementos básicos que la componen así como las funciones de cada una. En la Figura 1 se define los componentes y operación de red MPLS.

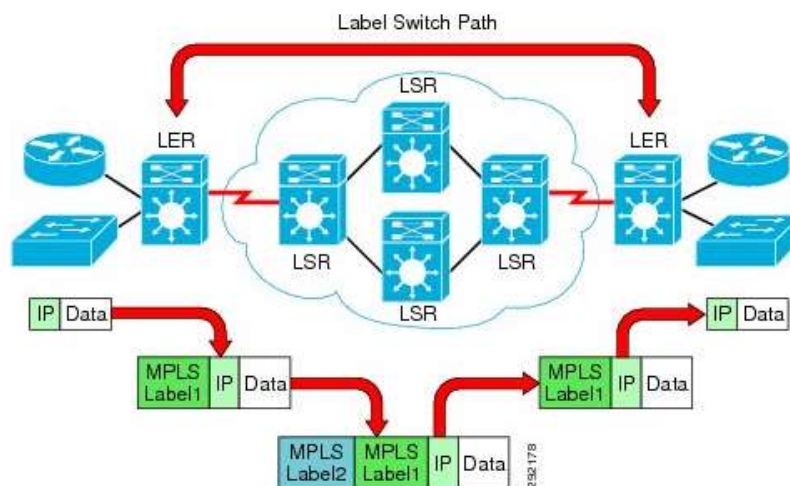


Figura 1. Componentes y operación de la red MPLS [11]

LSR (Label Switching Router) son dispositivos ubicados en el core de la red, encaminan los paquetes en función de la etiqueta MPLS. Al realizar la comparación con la red de CNT EP son los equipos de core que se detallara en la siguiente sección.

LER (Label Edge Router) son dispositivos ubicados en el extremo de la red, es decir equipos de entrada y salida de la red MPLS una de las funciones principales es iniciar o terminar el túnel (retira o coloca etiquetas). Al realizar una analogía son los equipos de distribución de la red de CNT EP

FEC (Forwarding Equivalence Class): conjunto de paquetes que entran en la red MPLS por la misma interfaz, que reciben la misma etiqueta y por tanto circulan por un mismo trayecto.

LDP (Label Distribution Protocol): es el protocolo que utilizan los dispositivos LSR para asignar las etiquetas.

LSP (Label Switched Path): Camino que siguen por la red MPLS los paquetes que pertenecen determinado tráfico o FEC.

5.1.3 Modelo Jerárquico

El modelo Jerárquico de tres capas es utilizado por CNT EP en el backbone IP/MPLS, en donde cada capa tiene funciones específicas, lo que simplifica el diseño y por lo tanto, la implementación y administración de la red.

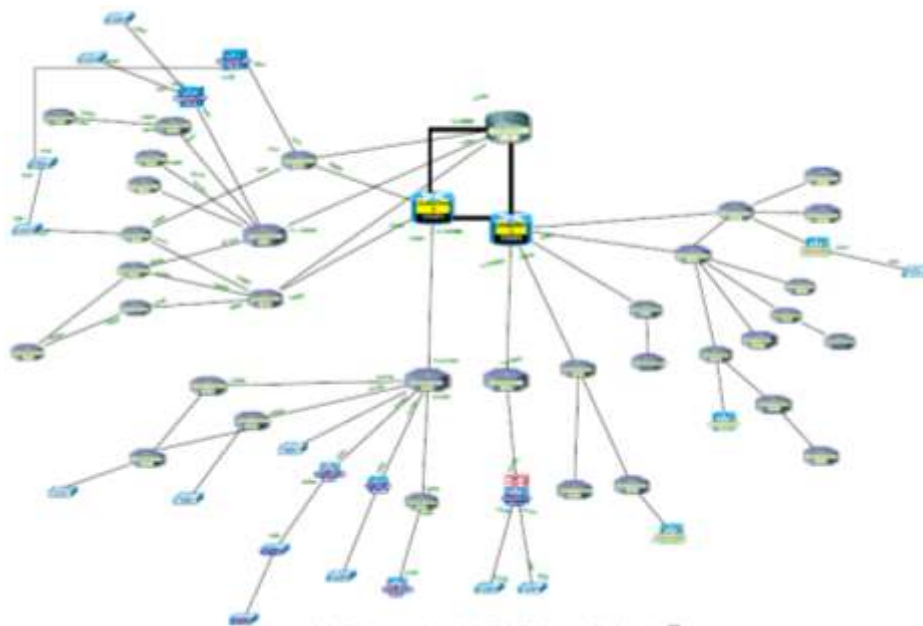


Figura 2. Nivel Jerárquico de CNT EP. [Elaborado por el autor]

Capa de núcleo o de Core.

La función principal es *switchear* el tráfico lo más rápido como sea posible y se encarga de transportar grandes cantidades de tráfico de manera confiable y veloz, por lo que la latencia y la velocidad son elementos importantes en esta capa. Tiene alta redundancia a nivel de enlace físico, igualmente dispone de redundancia a nivel de conexiones es decir si el equipo falla por completo la información está en otro equipo de Core P. A estos equipos de core se conectan equipos de distribución PE. CNT EP cuenta con 20 equipos de Core de marca Cisco. Las series de los equipos son: CRS-8/S, 12816/PRP y CRS-4/S distribuidos estratégicamente a nivel nacional.

En la Tabla 1 se detalla un ejemplo de los equipos de core con su nomenclatura y donde están ubicados.

Marca	NEMONICO	LOCALIDAD
CISCO	AMBSURP01	TUNGURAHUA AMBATO_SUR CRS-8/S
CISCO	CCACNTP01	AZUAY CUENCA_CENTRO 12816/PRP
CISCO	ESMPALP01	ESMERALDAS LAS_PALMAS 12810/PRP

Tabla 1. Equipos de Core de CNT EP. [Elaborado por el autor]

Capa Distribución

Los switch L3 de la Capa de distribución presenta alta disponibilidad y redundancia.

Entre las funciones principales se puede citar:

- Dotar de una comunicación entre la capa de Acceso y la de Core.
- Controlar el tráfico de la red utilizando políticas así como trazar los dominios de broadcast.
- Proveer las funciones de enrutamiento (*routing*), ya sea interno dentro de la red MPLS y enrutamiento hacia los clientes.

En la CNT EP en la capa de distribución utiliza dos tipos de equipos que los se denomina Tipo A y Tipo B.

Equipo Distribución o de Borde PE Tipo A:

Los equipos de distribución Tipo A son equipos ASR serie 9000 de marca Cisco XR que dispone de un sistema operativo XR.

Equipo Distribución o de Borde PE Tipo B:

Los nodos de distribución Tipo B corresponden a los modelos ME 3600, ME 3800, 7609-S, 7606-S de marca Cisco y tiene un sistema operativo IOS. En la Tabla 2 se observa ejemplo de los equipos de distribución.

Marca	NEMONICO	LOCALIDAD
CISCO	UIOINQE03	PICHINCHA IÃ‘AQUITO ASR9K
CISCO	AMBSURE01	TUNGURAHUA AMBATO_SUR CISCO7606-S

Tabla 2. Equipos de distribución de CNT EP. [Elaborado por el autor]

CNT EP cuenta aproximadamente con *540 equipos en la capa de Distribución* que se encuentra desplegado a nivel nacional.

Capa de Acceso

La capa de acceso es la interfaz de conexión con el cliente, CNT EP dispone de diferentes tecnologías para el acceso de Última milla como son: xDSL, xPON, Wimax, Radio-Enlaces, Fibra óptica Pto-Pto, redes celulares 2G, 3G, y 4G entre otras; los cuales se conectan a nodos (routers, switch) que están dentro la Red IP/MPLS, utilizando mecanismos de conmutación y transporte de VLANs basadas en 802.1Q y 802.1ad (QinQ) Se utiliza tres tipos de equipos de acceso denominados tipo A, tipo B y Tipo C.

- **Equipos de Acceso Tipo A**

Corresponde a los modelos C2960, ME 3400, ME 3600, ME 3560, ME3800X de marca Cisco, el sistema operativo es IOS

- **Equipos de Acceso Tipo B**

Son conmutadores de Marca Alcatel-Lucent del modelo OS6855-U24X con sistema operativo AOS. Aproximadamente se dispone de 150 equipos de esta marca.

- **Equipos de Acceso Tipo C**

Son conmutadores de marca Huawei de los modelo S5328C-EI-24S, S5624P, NE40E&80E, CX600-4. Se dispone de aproximadamente 270 equipos de acceso Tipo C.

CNT EP cuenta con alrededor de *1840 equipos de acceso* en la Red MPLS.

Nomenclatura de los equipos MPLS

Para identificar los equipos MPLS, y al nivel jerárquico que pertenece se utiliza la siguiente nomenclatura, el cual se divide en tres grupos ejemplo CCACPOZE01 donde:

El primer grupo.- tres primeras letras (**CCA**) indican la capital de la provincia donde está instalado el equipo en este caso CUENCA.

El segundo grupo 3 o 4 letras (**CPOZ**) se abrevia el cantón, parroquia, sector, o barrio, en este caso Camilo Ponce Enriquez.

Y el tercer Grupo (E01) indica el nivel Jerárquico y cuantos equipos están en el sector. Para los de equipos de core se utiliza la letra **P**, para los de distribución **E** y para los de acceso **M**. En la Tabla 3 se detalla algunos ejemplos de nomenclatura.

Marca	NEMONICO	LOCALIDAD	NIVEL JERÁRQUICO
CISCO	AMBSURP01	TUNGURAHUA AMBATO_SUR	Capa de Core
CISCO	AMBQEROE01	TUNGURAHUA QUERO	Capa de Distribución
CISCO	AMBPINLM02	TUNGURAHUA PINLLO_2	Capa de acceso

Tabla 3. Ejemplo de nomenclatura de los equipos MPLS. [Elaborado por el autor]

5.1.3 Configuración de los equipos de la red IP/MPLS de CNT EP

En la presente sección se detalla la configuración de protocolos utilizados para establecer conectividad en la red IP/MPLS. Se citara y verificara la configuración de los principales parámetros y protocolos (MPLS, LDP, BGP, IS-IS) que están habilitados en la red MPLS y permiten establecer la comunicación entre equipos.

Protocolo de Internet IPv4 en el Red MPLS

El protocolo de Internet utilizado en la red MPLS es IPv4, se aplica actualmente para proveer conectividad mediante direcciones IP a los clientes corporativos. De igual manera se emplea para aprovisionar direcciones IP a las interfaces de los equipos que forman parte de la Red IP/MPLS de CNT EP.

Para identificar a las interfaces de los equipos de la red se utiliza la dirección de red 10.X.X.X /8, a la cual se realiza subneting 10.X.X.X /30 para los enlaces entre equipos y 10.X.X.X /32 para interfaz de loopback.

Interfaz loopback

CNT EP utiliza interfaz virtual loopback en la configuración de los equipos, la cual es empleada para diferentes propósitos como: Router-ID, establecer sesiones BGP, interfaz de monitoreo de los equipos, entre otros. En la figura 3 se visualiza la configuración de la loopback en el equipo de Ambato-Huachi

```

AMBHCHJE01#sh running-config interface loopback 100
Building configuration...

Current configuration : 102 bytes
!
interface Loopback100
  description ### Router-ID ###
  ip address 10.3.44.100 255.255.255.255
end

```

Figura 3. Interfaz loopback en equipos de Red IP/MPLS. [19]

IP CEF

CNT EP al tener equipos de core y distribución marca Cisco se habilita el protocolo CEF (Cisco Express Forwarding) que es un feature y permite una conmutación más rápida en dispositivos de la marca en mención. Se basa en la tabla FIB (Base de información de envío) que contiene una información completa de conmutación IP. El ruteador utiliza la información de esta tabla para envío de paquetes, en la figura 4 se puede observar el protocolo activado en el equipo de Ambato-Huachi

```

AMBHCHJE01#sh ip cef
Prefix      Next Hop      Interface
0.0.0.0/0   no route
0.0.0.0/8   drop
0.0.0.0/32   receive
10.0.0.0/8   10.83.43.6    GigabitEthernet0/17
10.1.1.100/32 10.83.43.6    GigabitEthernet0/17
10.1.2.100/32 10.83.43.6    GigabitEthernet0/17
10.1.10.100/32 10.83.43.6    GigabitEthernet0/17
10.1.10.192/26 10.83.43.6    GigabitEthernet0/17
10.1.11.100/32 10.83.43.6    GigabitEthernet0/17
10.1.20.100/32 10.83.43.6    GigabitEthernet0/17
10.1.20.192/26 10.83.43.6    GigabitEthernet0/17
10.1.21.100/32 10.83.43.6    GigabitEthernet0/17
10.1.21.192/26 10.83.43.6    GigabitEthernet0/17
10.1.22.100/32 10.83.43.6    GigabitEthernet0/17
10.1.22.192/26 10.83.43.6    GigabitEthernet0/17
10.1.25.100/32 10.83.43.6    GigabitEthernet0/17
10.1.27.100/32 10.83.43.6    GigabitEthernet0/17
10.1.30.100/32 10.83.43.6    GigabitEthernet0/17
10.1.30.192/26 10.83.43.6    GigabitEthernet0/17
10.1.31.100/32 10.83.43.6    GigabitEthernet0/17
10.1.31.192/26 10.83.43.6    GigabitEthernet0/17
10.1.35.100/32 10.83.43.6    GigabitEthernet0/17
10.1.35.192/26 10.83.43.6    GigabitEthernet0/17
10.1.40.100/32 10.83.43.6    GigabitEthernet0/17
10.1.40.192/26 10.83.43.6    GigabitEthernet0/17
10.1.41.25/32 10.83.43.6    GigabitEthernet0/17
10.1.41.42/32 10.83.43.6    GigabitEthernet0/17

```

Figura 4. CEF habilitado en la Red MPLS CNT EP. [19]

Protocolo de Distribución de Etiquetas LDP

El Protocolo LDP propietario de cisco facilita los medios para que los equipos puedan solicitar distribuir, liberar la información de los prefijos de las etiquetas hacia los demás routers de la red.

```

AMBHCHJE01#sh mpls interfaces
Interface      IP      Tunnel  BGP  Static  Operational
GigabitEthernet0/1  Yes (ldp)  Yes    No    No    Yes
GigabitEthernet0/17 Yes (ldp)  Yes    No    No    Yes
TenGigabitEthernet0/1 Yes (ldp)  Yes    No    No    Yes
TenGigabitEthernet0/2 Yes (ldp)  Yes    No    No    Yes
Tunnel30211       No        No     No    No    Yes
Tunnel34412       No        No     No    No    Yes
AMBHCHJE01#sh run int GigabitEthernet0/1

```

Figura 5. LDP habilitado en la Red MPLS CNT EP. [19]

Protocolo de enrutamiento interno IS-IS (Intermediate system to intermediate system)

CNT EP como protocolo de enrutamiento interno utiliza IS-IS INTEGRADO para la distribución de Rutas. Las direcciones NSAP utilizadas es una modificación de la interfaz loopback configurada en los equipos.

Para formar las direcciones NET (Network Entity Title) que identifican al router en el proceso IS-IS se utiliza el AFI 49 que indica una dirección NSAP privada, se selecciona una área única que se identifica con 0001, después del área se coloca la dirección IP que lo

identifica, para esto se modifica la dirección de loopback aumentando 0 para completar la estructura de 6 bytes.

NET	Loop
49.0001.1720.3001.0020.00	172.30.10.20

La diferencia de las direcciones NET de IS-IS es que se lo utiliza para todo el router a diferencia del direccionamiento estilo IP que se utiliza una dirección para cada interfaz.

```

router isis 1
 net 49.0001.1720.3001.0020.00
 is-type level-2-only
 authentication mode mdf level-2
 authentication key-chain IS5
 ispf level-2
 metric-style wide
 fast-rload 15
 ip route priority high tag 20
 set-overload-bit on-startup 180
 max-hp-lifetime 65535

```

Figura 6. Configuración IS-IS en red MPLS de CNT. [19]

Protocolo de Puerta de Enlace de Borde (BGP)

CNT EP tiene configurado el protocolo BGP para intercambiar rutas entre clientes y otros proveedores de servicios. Cuando BGP se utiliza para aprender rutas de diferentes sistemas autónomos (AS) se hace referencia a external BGP (EBGP), y cuando se aprende rutas del mismo sistema autónomo se hace referencia a internal BGP (iBGP) este permite conocer redes de los clientes que se configuraron mediante redes privadas virtuales (VPN).

El número de proceso BGP es 28006 se encontrará configurado en los equipos que conforman la red MPLS.

```

router bgp 28006
|
address-family ipv4 vrf dat2432
  redistribute connected
  redistribute static
exit-address-family

```

Figura 7. Proceso 28006 de BGP de CNT EP. [19]

Calidad de Servicio QoS

CNT EP ofrece prioridad a determinados tipos de tráfico que pasan por la red, ya que son necesarios cuando se ofrece servicios en tiempo real como la voz. De manera general la Calidad de Servicio que se tiene implementado ayuda a priorizar los diferentes servicios que se entrega a los clientes. Básicamente tiene creado 6 clases-map en toda la red IP/MPLS en donde la Clase VoIP se define como prioritaria. En la Tabla 4 se detalla los class-map creados

Clases
CM – VoIP 10%
CM - Controlred
CM-Video 20%
CM-Datoscritico 20%
CM-Datosnocirticos
Default 3%

Tabla 4. Class-Map de CNT EP. [Elaborado por el autor]

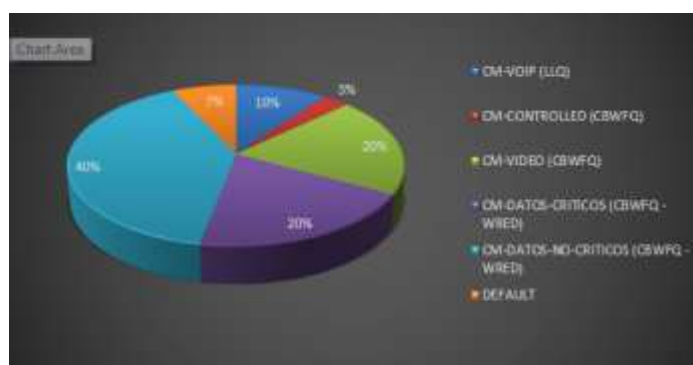


Figura 8. Class-Map de CNT EP. [Elaborado por el autor]

En la figura 9 y figura 10 se puede observar los class-map creado en uno de los equipos MPLS (Quito-Mariscal) y su respectiva configuración.


```

UIOMSCE01#show policy-map PM-QoSBB
Policy Map PM-QoSBB
Class CM-VoIP
  priority
  police rate percent 10
    conform-action transmit
    exceed-action drop
Class CM-Controlred
  bandwidth 3 (%)
Class CM-Video
  bandwidth 20 (%)
Class CM-Datoscriticos
  bandwidth 20 (%)
  packet-based wred, exponential weight 9

```

Figura 9. Class-Map en equipo de Distribución de Mariscal [19]

```

UIOMSCE01#sh class-map CM-Controlred
Class Map match-any CM-Controlred (id 5)
Match mpls experimental topmost 6 7
Match precedence 6 7

UIOMSCE01#sh class-map CM-Video
Class Map match-any CM-Video (id 23)
Match mpls experimental topmost 4
Match precedence 4

UIOMSCE01#sh class-map CM-Datoscriticos
Class Map match-any CM-Datoscriticos (id 24)
Match mpls experimental topmost 3
Match precedence 3

UIOMSCE01#sh class-map CM-Datosnocriticos
Class Map match-any CM-Datosnocriticos (id 2)
Match mpls experimental topmost 1 2
Match precedence 1 2

UIOMSCE01#sh class-map class-default
Class Map match-any class-default (id 0)
Match any

```

Figura 10. Configuración Class-Map en equipo de Distribución de Mariscal. [19]

Entre las políticas que se encuentran implementadas están:

- Definición de la clase CM-VoIP como prioritaria
- Limitación del tráfico en la cola prioritaria al 10% del ancho de banda
- Asignación de ancho de banda mínimos. Ver tabla 4.
- Descarte de tráfico aleatorio mediante mecanismo para evitar congestión WRED (*Weighted Random Early Detect Distribute*) en las clases: Datoscriticos, Datosnocriticos y class-default.

Estas configuraciones pueden variar de acuerdo a los requerimientos o necesidades del cliente, se brinda las facilidades para priorizar el tráfico que el cliente desee en su enlace de datos.

5.1.4 Configuración de Clientes Corporativos en la Red IP/MPLS de CNT EP

Los clientes corporativos y/o gubernamentales que contratan servicios como Datos, Internet, Telefonía IP, se configura en la red MPLS a nivel de capa 3, con las direcciones IPv4 (públicas o privadas). Cada servicio segmentado utiliza una instancia de enrutamiento o VRF **Virtual Routing and Forwarding**, de esta manera se tiene:

VRF netcnt/netdef : utilizada para clientes corporativos y/o gubernamentales para servicio de internet. Se asocian direcciones IPv4 Publicas.

VRF voipXXXX: utilizada para clientes corporativos y/o gubernamentales para servicio de telefonía IP. Se asocian direcciones IPv4 Privadas únicas para cada cliente.

VRF datXXXX: utilizada para clientes corporativos y/o gubernamentales para servicio de Datos. **Se crea una vrf para cada cliente.** Generalmente se utiliza direccionamiento IP privado

La VRF permite la creación de múltiples tablas de enrutamientos dentro del mismo router, lo que puede existir superposición de direcciones IP de diferentes clientes.

Para configurar un cliente corporativo con su VRF se realiza el siguiente procedimiento:

Configuración de la VRF

Dentro del proceso BGP 28006 se configura la instancia de enrutamiento VRF

Nombre de la VRF (datXXXX)

Route distinguisher : se ingresa el número de sistema autónomo y el número de piloto o identificador del cliente .

Route Target: Crea una lista de comunidades para el destino de la ruta.

```
Current configuration : 441 bytes
ip vrf dat2432
rd 28006:202432
route-target export 28006:202432
route-target import 28006:202432
```

Figura 11. Configuración de VRF de un cliente. [19]

Configuración Red Privada Virtual (VPN) en MPLS

CNT EP utiliza su infraestructura para proporcionar conectividad entre los sitios de los clientes utilizando VPN permitiendo que estos sitios tengan visibilidad entre ellos. [9] Se utiliza el protocolo MPLS como medio de transporte para poder crear túneles entre los sitios del cliente. La VPN capa 3 se configura en los *routers de borde* (*Router Provider Edge PE*) en donde se generan tablas de ruteo especiales para separar las rutas privadas de los clientes de las rutas del proveedor. Los routers o equipos PE anuncian estas rutas específicas utilizando sesiones Multiprotocol BGP (MP-BGP) a otros PE en donde la VPN tenga presencia [9].

Para que la tabla de enrutamiento y la VRF del cliente se propague dentro de la red IP/MPLS, se configura dentro del proceso BGP un **address-family ipv4** que indica cómo distribuir las rutas, adicional a esto se configura **address-family vpnv4** que representa el túnel que se levanta entre los equipo PE a través de MPLS.

```
router bgp 28006
!
address-family ipv4 vrf dat2432
 redistribute connected
 redistribute static
 exit-address-family
```

Figura 12. Address family en BGP 28006. [19]

Configuración de Direccionamiento IP en la Interfaz.

En esta parte se configura el direccionamiento IP que utilizará el cliente y se lo asocia a una interfaz ya sea física o virtual. De lado del proveedor de servicio se configura en el equipo de distribución PE a nivel de capa 3 con los siguientes parámetros.

- **IP_WAN** Generalmente /30, una IP del lado de MPLS y la otra IP en el CPE del cliente
- **IP_LAN:** Generalmente /24 varía en base a los requerimientos del cliente.

Para internet corporativo se utiliza IPs Públicas /29.

- **IP VRF forwarding:** la VRF que se crea para el cliente corporativo se añade a la correspondiente interfaz, generalmente en CNT EP se le asocia a la VLAN. Existen casos esporádicos en donde el equipo de acceso es a su vez distribución, en estos casos la VRF se asocia a la interfaz física

En la figura 13 se visualiza la configuración de servicio de datos de cliente corporativo

```
interface Vlan935
description 896014
ip vrf forwarding dat2432
ip address 10.10.10.9 255.255.255.252
!
ip route vrf dat2432 10.0.3.0 255.255.255.0 Vlan935 10.10.10.10
end
```

Figura 13. Configuración de interfaz VLAN asociado a VRF. [19]

5.1.5 Resumen de la situación actual de Red IP/MPLS CNT EP

En la Tabla 5 se presenta un resumen de los protocolos básicos utilizados en la configuración actual de la Red, que servirá de base para poder realizar el análisis del método migración de coexistencia entre IPv4 / IPv6.

Protocolo	Descripción/Característica
Nivel Jerárquico	<p>Utiliza modelo de tres capas de cisco.</p> <p>Capa de Core. CRS-8/S, 12816/PRP y CRS-4/S marca cisco. Dispone de 20 equipos de Core</p> <p>Capa de Distribución. 7609-S , 12000/10 y 12000/16 de marca Cisco. Aproximadamente 540 equipos</p> <p>Capa de acceso : modelo 7606-S , ME6524, ME3800X marca cisco. Aproximadamente 1840 equipos</p>
Protocolo de Internet IPv4	<p>Se utiliza enrutamiento interno IPv4 para establecer conectividad en la Red IP/MPLS.</p> <p>Utiliza la 10.X.X.X para configuración interna de la red</p> <p>Direcciones IPv4 para servicios a clientes corporativos</p>
Interfaz loopback	Se utiliza interfaz virtual con varios propósitos, ID_Router, sesiones BGP, interfaz para monitoreo de equipos entre otros
Protocolo en enrutamiento Interno IS-IS	El protocolo enrutamiento interno es IS-IS
Protocolo BGP	<p>Numero de Proceso 28006.</p> <p>Establecer conectividad con clientes mediante el uso de EBGP. Permite configurar MPLS-VPN</p>
Protocolo LDP	Utilizado para la distribución de etiquetas en la red MPLS
IP MPLS	Protocolo de etiquetas. Habilitado en las interfaces
Protocolo CEF	Protocolo propietario de Cisco, facilita una conmutación más rápida de MPLS en equipos de la marca en mención.
Calidad De Servicio QoS	Básicamente tiene configurado 6 class-map para priorizar, voz, video, datos, control de red
Instancias de enrutamientos VRF	<p>Utilizado para clientes corporativos.</p> <p>Se encuentra configurado en los router de borde PE de la Red MPLS</p>

Tabla 5. Resumen de la situación actual de RED/IP MPLS de CNT EP. [Elaborado por el autor]

5.2 MÉTODOS DE MIGRACIÓN & COEXISTENCIA DE IPV4 E IPV6

Uno de los principales puntos a considerarse como problema en la transición de IPv4 a IPv6 radica en el hecho que los protocolos en mención son incompatibles entre sí. Se han desarrollado diferentes tecnologías con el objetivo de permitir o facilitar la transición/coexistencia de los protocolos, los cuales se analizarán básicamente pero aportando elementos que permitan comprender el principio de funcionamiento, este trabajo no pretende abordar todas las técnicas que existen ya que su cantidad es elevada.

La transición entre los protocolos IPv4 / IPv6 será un proceso que tomara tiempo, por lo que existirá un periodo donde coexistan ambos protocolos. Para una coexistencia de IPv4 e IPv6 la IETF creo varias técnicas que básicamente pueden dividirse en tres categorías.

Pila Doble “Dual Stack”.- conceptualmente es la manera más fácil de introducir IPv6 en una red, en este método un host o nodo tendrá ambas pilas de protocolo IPv4 e IPv6 provistas directamente como un componente del sistema operativo. Cada nodo se configura con ambas direcciones. El reto para el despliegue de una red Dual stack es la configuración de ruteo externo como interno para ambos protocolos, otro punto a tomar en consideración es que se debe disponer de suficientes direcciones IPv4 para desplegar las dos versiones del protocolo.

Tunneling : Es un método para transportar paquetes IPv6 a través de redes IPv4. Este mecanismo puede usarse cuando dos redes que usan el mismo protocolo desean comunicarse sobre una red que utiliza otro protocolo.

El proceso de tunel tiene tres pasos: encapsulamiento, desencapsulamiento, y administración del tunel. Se necesita dos extremos del túnel que se ocupan del encapsulamiento y desencapsulamiento los cuales generalmente son nodos que tiene implementado Dual Stack IPv4/IPv6.

Traducción: la traducción de direcciones de red 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado

mediante una técnica de traducción similar a la NAT para IPv4. Un paquete IPv6 se traduce en un paquete IPv4, y viceversa.

5.2.1 Métodos de migración y coexistencia de IPv4 / IPv6 sobre red

IP/MPLS

Para definir los métodos que mejor se ajustan a las necesidades de CNT EP se considera:

- La Red de CTN EP utiliza protocolo MPLS el cual está configurado en los equipos de borde y core.
- Utiliza direccionamiento IPv4 para establecer conectividad entre equipos que forman la red.
- Tiene habilitado protocolo BGP y IS-IS el cual es compatible con diferentes protocolos capa 3.

Tomando en consideración las características de la red existen tecnologías de túnel que permiten implementar IPv6 sobre MPLS sin alterar el core de la Red.

Básicamente se define los siguientes mecanismos para IPv6 sobre MPLS:

- IPv6 sobre circuitos de Transporte MPLS
- IPv6 con Túneles en los equipos de borde del cliente CE (IPv6 - **CE**)
- IPv6 sobre MPLS en los equipos de borde del proveedor (Provider Edge PE - **6PE**)
- IPv6 sobre MPLS-VPN en los equipos de borde del proveedor (**6VPE** – VPN - Provider Edge)

5.2.1.1 IPv6 sobre circuitos de transporte MPLS

Utilizando cualquier circuito de transporte para implementar IPv6 sobre redes MPLS no requieren cambios en los equipos de core del proveedor de servicios.

En este método se crean interfaces dedicadas mediante circuitos estáticos configurados sobre MPLS. La comunicación IPv6 entre los equipos de borde del cliente **CE** se realiza sobre enlaces dedicados y la ejecución nativa de IPv6, mediante túneles de capa 2 (ejemplo tecnologías Frame Relay, ATM, Ethernet) configurados en los equipos de borde del

proveedor de servicios **PE** , los cuales son encapsulados en MPLS y transportadas mediante etiquetas.

Es un mecanismo es estático fácil de implementar pero no es escalable generando problema cuando la red empieza a crecer

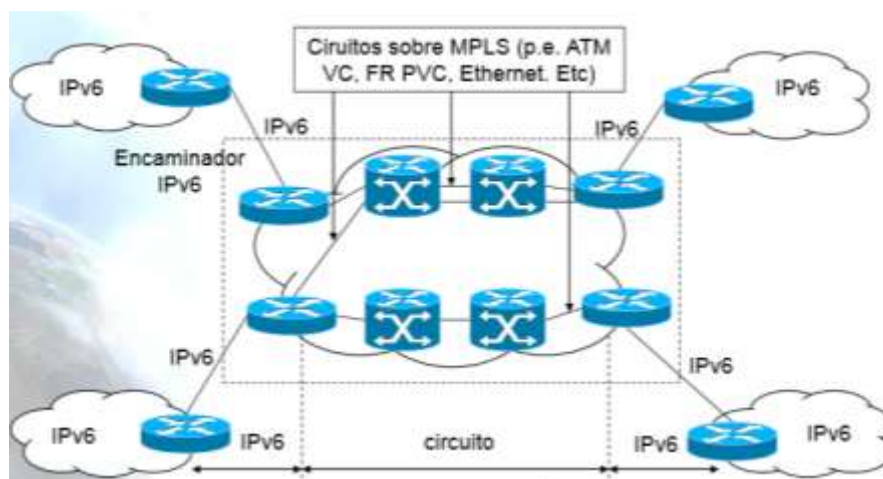


Figura 14. IPv6 sobre circuitos de transporte sobre MPLS [12]

5.2.1.2 IPv6 con túneles en los routers CE

Es una de las maneras más sencillas de integrar IPv6 sobre MPLS sin impacto en la operación o infraestructura de la red MPLS/IPv4 ya que no se ve alterada su configuración. Se implementa túneles tradicionales en cada uno de los routers de borde del cliente CE. Los equipos CE requieren ser dual Stack (doble pila) para soportar IPv4 e IPv6.

Los paquetes IPv6 se encapsulan con encabezados IPv4 para ser transportados a través de tuneles en la Red MPLS/IPv4. Se requiere un túnel entre cada CE que este implantado IPv6 (Full mesh), por lo que si la red es muy grande el número de tuneles a implementarse es proporcional, presentándose aquí la principal desventaja la escalabilidad.

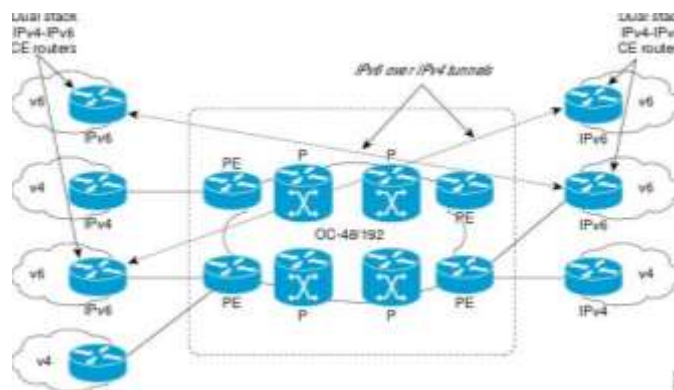


Figura 15. IPv6 con túneles en los routers CE [5]

5.2.1.3 Provider Edge 6PE - IPv6 sobre MPLS en los equipos de borde del proveedor PE

Este mecanismo permite transportar IPv6 a través de la red MPLS utilizando el protocolo BGP. Cuando BGP soporta IPv4 e IPv6 se lo conoce como *Multiprotocol – Border Gateway Protocol (MP-BGP)*. Los routers de borde del proveedor PE deben soportar IPv4 e IPv6 (Dual Stack). En esta solución los equipos de borde del proveedor PE de ingreso tienen una jerarquía de etiquetas para que el tráfico IPv6 sea transparente para los routers de core.

- La primera etiqueta (MPLS Label) provee conectividad o realiza el intercambio de etiquetas dentro del core MPLS/IPv4 la cual se distribuye por LDP, TDP, RSVP, o MPLS-TE,
- segunda etiqueta (MP-IBGP Label) establece comunicación interna en la nube utilizando protocolo IGP ejemplos OSPF o IS-IS. La interfaz de los routers de borde 6PE se conecta a los equipos de borde del cliente CE y pueden ser configurados para enviar tráfico IPv4, IPv6 o ambos dependiendo de los requerimientos del cliente
- 6PE conecta todas las redes IPv6 a través de una única VPN por lo que no pueden ser separadas lógicamente, para poder realizar dicha separación se utiliza 6VPE.

En la Figura 16 se observa la topología de método 6PE, este método se encuentra en el RFC 4798

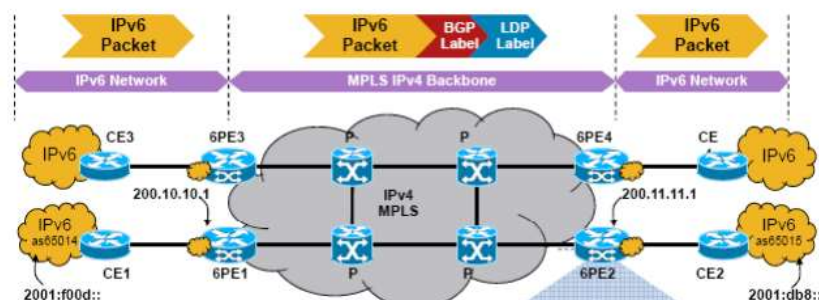


Figura 16. Topología de método 6PE [8]

5.2.1.4 Método 6VPE - IPv6 VPN sobre MPLS en los equipos de borde del proveedor PE

Posee las mismas características que el método 6PE, con la diferencia que *puede definir varias redes virtuales VPN utilizando instancias de enrutamiento VRF (Virtual Routing and Forwarding)*, para segmentar los diferentes servicios que ofrece el proveedor.

La operación de la VPN se divide básicamente en dos componentes:

- **Enrutamiento de Core** permite conectividad entre el equipo de borde del proveedor PE y el equipo de core, utiliza un protocolo IGP tales como OSPF o IS-IS.
- **Enrutamiento de Borde** se lleva a cabo en dos sentidos entre los pares PE y entre los equipos de borde del proveedor PE - y el equipos de borde del cliente CE. En la sección de los pares PE se utiliza el protocolo iBGP el cual aprende las rutas del CE y del PE-CE. En la sección de los PE-CE utilizan eBGP y VRF para establecer comunicación con el CE

Las principales ventajas del 6PE y 6VPE mantiene el Core MPLS intacto minimizando costos de implementación y perseverando la escalabilidad. Brinda flexibilidad (implementación gradual), permite aprovechar funcionalidad avanzadas de MPLs (TE, QoS etc), permite integrar IPv6 nativo, no es un esquema de traducción.

En la figura 17 se observa funcionamiento 6VPE, este método se encuentra en el RFC 4659

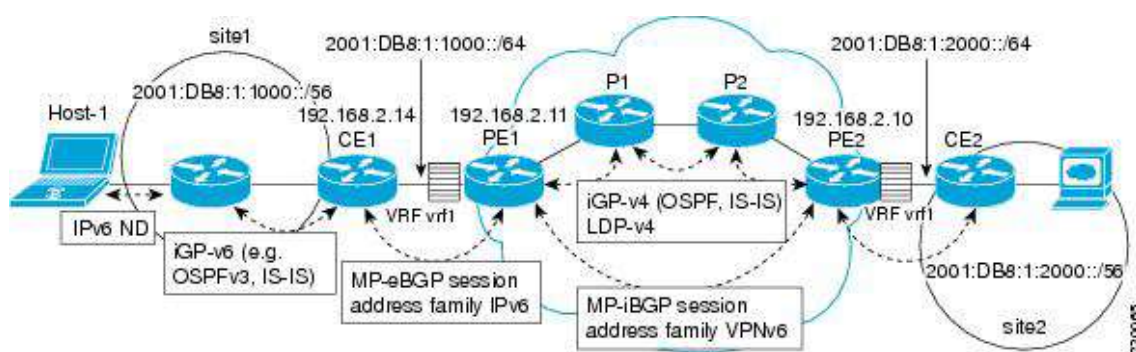


Figura 17. Funcionamiento método 6VPE [5]

5.2.2 Resumen de métodos de migración.

Luego de analizar los métodos de IPv6 sobre MPLS, se ha desarrollado la Tabla 6 con un resumen y principales características de cada método, lo que servirá de base para seleccionar el mejor mecanismo que se acople a las necesidades de CNT EP.

METODOS DE IPV6 SOBRE MPLS					
Método	Descripción	Cambios en la Red	Equipo Dual Stack	Ventaja	Desventaja
IPv6 sobre circuitos de Transporte en MPLS	La conectividad entre CE se realiza sobre enlaces dedicados mediante tuneles capa 2	Sin cambios en infraestructura de CORE	equipos CE	Mecanismo Fácil de implementar	No es escalable
IPv6 con túneles en los routers CE	Se configura tuneles de capa 3 en los equipos CE IPv6	No se realiza cambios en los equipos de core ni en los de borde PE	equipos CE	Mecanismo Fácil de implementar. No requiere cambios en el la Red MPLS.	No es escalable Se requiere un túnel entre cada CE. Configuración Manual de tuneles.
6PE	Utiliza el protocolo MP-BGP para el transporte de paquetes IPv6.	No se realiza cambios en los equipos de core ni en los de borde PE	equipos PE y CE	Flexibilidad (implementación gradual) Permite entregar IPv6 nativo al CE. No es esquema de Traducción.	6PE no soporta redes virtuales VPN. Tabal de enrutamiento global en el router del proveedor No soporta VRF.
6VPE	Utiliza el protocolo MP-BGP para el transporte de paquetes IPv6.	No se realiza cambios en los equipos de core. Verificar que equipo de borde soporte método.	equipos PE y CE	Soporta VPN. Se puede definir varias instancias de enrutamiento VRF Permite entregar IPv6 nativo al CE. No es esquema de Traducción. Implementación gradual de IPv6	Habilitación manual del envío de etiquetas BOTTOM generadas por MP-BGP.

Tabla 6. Resumen de métodos de IPv6 sobre MPLS. [Elaborado por el autor]

5.3 PROPUESTA DEL MÉTODO DE MIGRACIÓN Y COEXISTENCIA IPV4 & IPV6 SOBRE RED IP/MPLS DE CNT EP

En la sección 5.2 se realizó un análisis de los diferentes métodos de migración y coexistencia de IPv6 sobre MPLS y en la sección 5.1 se revisó la situación actual de Red de CNT EP. Con estos antecedentes se ha desarrollado la Tabla 7 donde se detalla las características para determinar la que mejor método de migración y coexistencia de IPv4 & IPv6 que se ajuste a las necesidades de CNT EP.

ANALISIS PROPUESTA PARA METODO PARA MIGRACION DE IPv4 a IPv6				
	IPv6 sobre circuitos de Transporte en MPLS	IPv6 con tuneles en los routers CE	IPv6 Provider Edge 6PE	IPv6 Virtual Provider Edge 6VPE
Métodos de Migración IPv6 sobre MPLS				
Equipos CE Dual Stack	SI	SI	SI	SI
Equipo PE Dual stack	NO	NO	SI	SI
Configuración de VRFs para proveer diferentes servicios	NO	NO	NO	SI
Escalabilidad para crecer redes de los clientes	NO	NO	SI	SI
Situación Actual de la Red MPLS de CNT EP				
Compatible Protocolos de enrutamiento IGP - IS-IS	SI	SI	SI	SI
Se mantiene configuración de los equipo core de MPLS	SI	SI	SI	SI
Se mantiene configuración de los equipo PE de MPLS	SI	SI	NO	NO
Compatible con protocolo BGP	SI	SI	SI	SI
Compatible configuración de VRF	NO	NO	NO	SI
Compatible con configuración QoS	SI	NO	SI	SI

Tabla 7. Características de métodos de migración en base a la situación actual de la Red.
[Elaborado por el autor]

Con base a la tabla 7 se determina que el mejor método que se ajusta actualmente a las necesidades de CNT EP es **IPv6 Virtual Provider Edge 6VPE**, ya que aprovecha las ventajas del protocolo BGP y MPLS, los cuales CNT EP tiene configurado para su funcionamiento actual, adicional permite levantar tuneles MPLS-VPN y configurar instancias de enrutamientos VRF para segmentar los servicios de los clientes, es decir las características son muy similares a la que se tiene configurado actualmente. En los próximos ítems se analizara los cambios de hardware, software y configuraciones lógicas que intervienen en el método propuesto.

5.3.1 Análisis de requerimientos de Hardware y Software para la migración / coexistencia

Con el método seleccionado 6VPE uno de los principales impactos es que los equipos de borde del proveedor PE de la red MPLS deben soportar Dual Stack, VRF, VPN capa 3, QoS, direccionamiento IPv4 e IPv6 por lo que se analiza la marca, versión del equipo, software, versión del sistema operativo y se valida que soporte la configuración de 6VPE.

CNT EP tiene 540 equipos PE de la marca Cisco de las siguientes series ASR serie 9000, con IOS XR, series ME 3600, ME 3800, 7609-S, 7606-S que tiene un sistema operativo IOS. EN LA Figura 18 se utiliza el comando show versión para obtener información del equipo.

```

NVLONT01#sh ver
Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIPSERVICESK9-M), Version 12.2(33)SR6, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 15-Mar-12 04:46 by prod_rel_team

ROM: System Bootstrap, Version 12.2(33r)SR05, RELEASE SOFTWARE (fc1)
BOOTLDR: Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIPSERVICESK9-M), Version 12.2(33)SR6, RELEASE SOFTWARE

NVLONT01 uptime is 2 years, 47 weeks, 2 days, 16 hours, 6 minutes
uptime for this control processor is 2 years, 47 weeks, 2 days, 12 hours, 43 minutes
System returned to ROM by reload (SP by reload)
System restarted at 05:43:13 UTC Fri Apr 5 2013
System image file is "bootdisk:/c7600rsp72043-advipservicesk9-mz.122-33.SR6.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.

```

Figura 18. Comando show versión para obtener información del equipo. [19]

En la Tabla 8 se realiza un resumen de los equipos de borde PE con sus características de hardware/software.

Hardware/ series	ASR-9010	ME 3600	ME-3800X	7609-S	7606-S	A901
Número de equipos	18	80	337	43	20	42
Software IOS	XR 4.3.1	15.3(3)S2	15.3(3)S2	12.2(33)SRE6	12.2(33)SRE6	15.3(3)S

Tabla 8. Equipos PE de CNT EP Hardware y software. [Elaborado por el autor]

Como se observa existen 18 equipos ASR que son muy robustos en cuanto a características de hardware y software permitiendo soportar grandes cantidades de tráfico. Estos equipos se encuentran ubicados estratégicamente donde el volumen de enlaces y datos es mayor como por ejemplo en Pichincha sector la Mariscal, Guayas sector Bellavista etc. En el gráfico 16 se verifica porcentualmente la relación que existe entre los equipos PE, los mismos han sido ubicados en diferentes Provincias, ciudades, sectores previos análisis volumen de tráfico

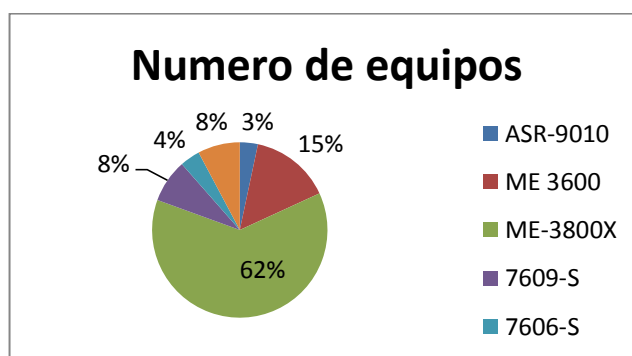


Figura 19. Número de Equipos de Distribución por serie. [Elaborado por el autor]

En la Tabla 9 se analizaron los equipos de borde PE que dispone CNT EP y los protocolos que soporta. Se puede verificar que todos los equipos que actualmente dispone CNT EP soportan la configuración del método 6VPE.

HW / SW IOS	Características	6VPE
ASR-9010 / XR 4.3.1	Soporta MPLS, MPLS VPN, EoMPLS IPv4 / IPv6 Routun (OSPF, EIGRP, RIP, IS-Is, BGP) IPv6 VPN sobre MPLS, IPv6 ACL QoS, QoS basado en Vlan CoS Otros Protocolos, STP, MSTP, HSRP, VRRP, ACL, SNMP etc	si
A901 / 15.3(3)S	Soporta MPLS, MPLS VPN, EoMPLS IPv4 / IPv6 Routun (OSPF, EIGRP, RIP, IS-Is, BGP) IPv6 VPN sobre MPLS, IPv6 ACL QoS, QoS basado en Vlan CoS Otros Protocolos, STP, MSTP, HSRP, VRRP, ACL, SNMP etc	si
ME 3600 / 15.3(3)S2	Soporta MPLS, MPLS VPN, EoMPLS IPv4 / IPv6 Routun (OSPF, EIGRP, RIP, IS-Is, BGP) IPv6 VPN sobre MPLS, IPv6 ACL QoS, QoS basado en Vlan CoS Otros Protocolos, STP, MSTP, HSRP, VRRP, ACL, SNMP etc A nivel de Hadware tien 24 puertos GE Electricos	si
ME-3800X / 15.3(3)S2	Soporta MPLS, MPLS VPN, EoMPLS IPv4 / IPv6 Routun (OSPF, EIGRP, RIP, IS-Is, BGP) IPv6 VPN sobre MPLS, IPv6 ACL QoS, QoS basado en Vlan CoS Otros Protocolos, STP, MSTP, HSRP, VRRP, ACL, SNMP etc A nivel de Hardware tien 24 puertos GE SFP	si
7609-S / 12.2(33)SRE6	Soporta MPLS, MPLS VPN, EoMPLS IPv4 / IPv6 Routun (OSPF, EIGRP, RIP, IS-Is, BGP) IPv6 VPN sobre MPLS, IPv6 ACL QoS, QoS basado en Vlan CoS Otros Protocolos, STP, MSTP, HSRP, VRRP, ACL, SNMP etc	si
7606-S / 12.2(33)SRE6	Soporta MPLS, MPLS VPN, EoMPLS IPv4 / IPv6 Routun (OSPF, EIGRP, RIP, IS-Is, BGP) IPv6 VPN sobre MPLS, IPv6 ACL QoS, QoS basado en Vlan CoS Otros Protocolos, STP, MSTP, HSRP, VRRP, ACL, SNMP etc	si

Tabla 9. Características de los equipos PE de CNT. [Elaborado por el autor]

5.3.2 Análisis de tráfico en la red IP/MPLS con IPv6

Para el estudio se toma en consideración el tráfico actual con IPv4 que está cursando entre los equipos de borde PE y los equipos de core, se analizó el tráfico de estas interfaces ya que es donde concentra el tránsito de los datos de varios clientes.

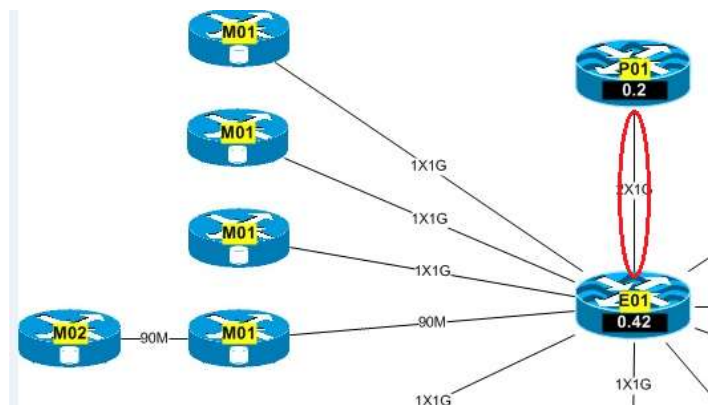


Figura 20. Trafico en interfaz de Equipo PE – P. [Elaborado por el autor]

La obtención de los datos estadísticos de tráfico se recolecto del sistema de monitoreo que dispone CNT EP en esta caso CACTI, donde brinda información del trafico entrante, máximo, promedio, trafico saliente máximo promedio, durante un periodo 4 semanas.

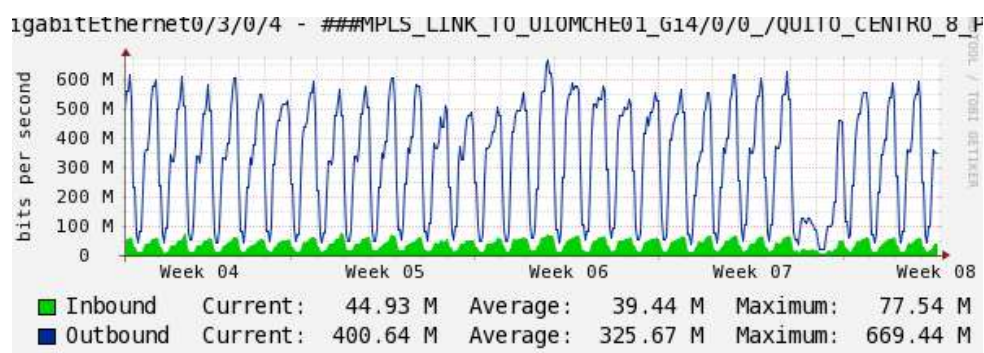


Figura 21. Trafico del equipo UIOQCNP01 – UIOMCHE01. [18]

En la figura 21 se visualiza el tráfico desde el equipo de borde PE de MACHACHI al equipo de core P de QUITOCENTRO, teniendo tráfico entrante promedio de 39.44M y Máximo de 77.54M, igualmente Trafico Saliente Promedio de 325.67M y Máximo de 669.44M.

Tráfico Total en la interfaz = Trafico Promedio Entrante + Trafico Promedio saliente

Tráfico Total en la interfaz = 39.44 + 325.67

Tráfico Total en la interfaz = 365.11 Mbps

Tramas Ethernet en la Interfaz = Tráfico total de la interfaz / (1500*8 bits)

Tramas Ethernet en la Interfaz = 365*000.000/ 12000

Tramas Ethernet en la Interfaz= 30.416 Tramas x segundo

Con estos resultados se obtienen el tráfico y las tramas que están actualmente cursando con IPv4. El objetivo es verificar el incremento de tramas cuando entre en funcionamiento el método propuesto 6VPE por lo que cabecera IPv6 se aumenta en 20 bytes.

Tramas generadas con IPv6 (20 bytes extras) = $20 \times 30.416 = 608320$

Tráfico Total para IPv6 = $(608320 \times 8) + 365\,000\,000$ bits

Tráfico Total para IPv6 = $4.866.560 + 365\,000\,000 = 369,9$ Mbps

Luego de los cálculos se determina que el aumento de tráfico en la interfaz es mínimo, aproximadamente 4.9 Mbps, lo que no afecta en la capacidad de transmisión ya que por una parte las interfaces de conexión de los equipos son Giga y los sistemas de Transmisión que utiliza CNT EP brinda la facilidad de poder crecer, sin que este aumento represente un impacto en dichos sistemas.

Con el objetivo de realizar una estadística realista sobre el incremento de tráfico en las diferentes interconexiones de los equipo PE - P, se adjunta varias gráficas y se realiza un resumen con los principales nodos donde se concentra mayor tráfico de clientes y se detallara el valor aumentarse en cada uno de ellos.

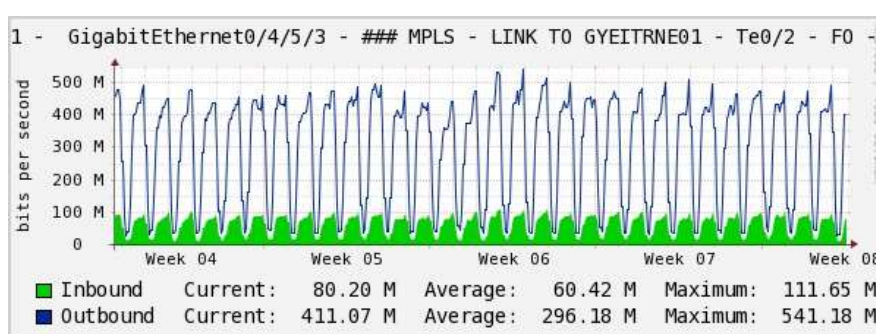


Figura 22. Isla Trinitaria Pe – Guayaquil P. [18]

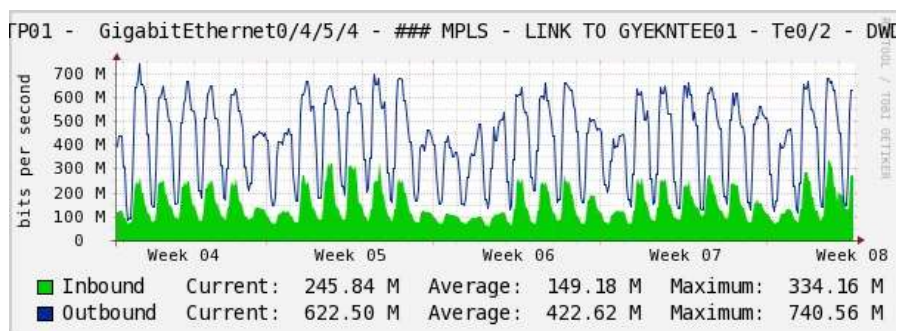


Figura 23. Guayaquil Kennedy PE – Guayaquil P. [18]

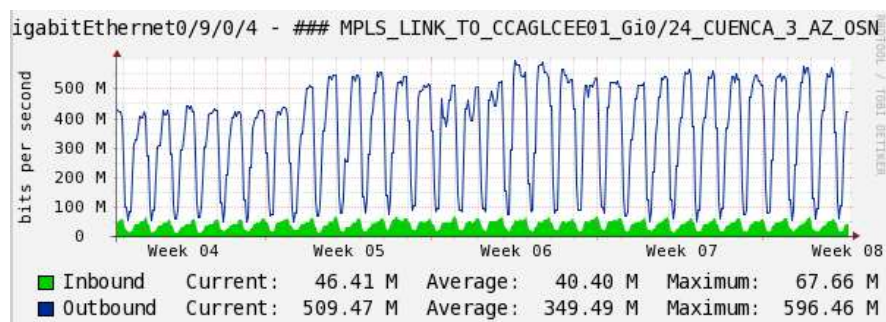


Figura 24. Cuenca Gualaceo PE – Cuenca P. [18]

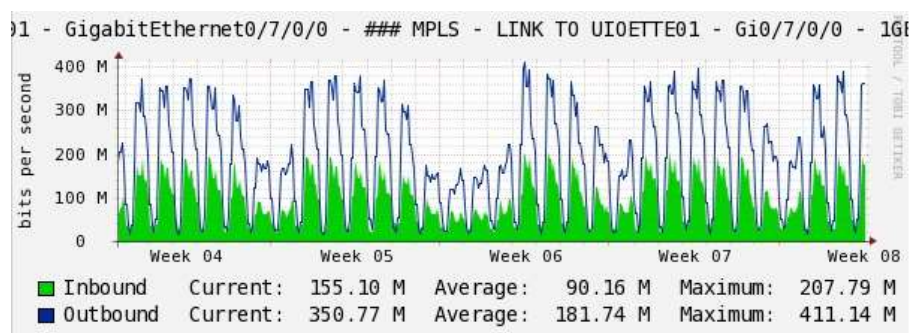


Figura 25. Estación Terrena PE – Quito Centro P. [18]

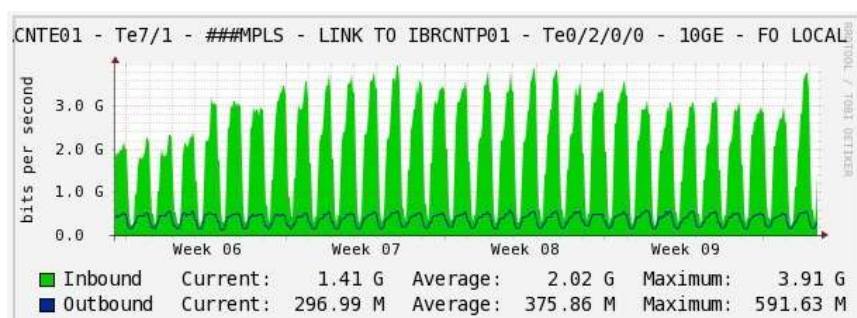


Figura 26. Ibarra Centro PE – Ibarra P. [18]

En la Tabla 10 se resume el cálculo realizado anteriormente para determinar el número de Tramas IPv6 que pasara por las interfaz de interconexión entre los equipos PE – P, se tomara

una muestra de 21 interfaces. Adicional se indica Trafico Promedio que aumentara con IPv6.

Con esto se ratifica que el incremento de tráfico es mínimo.

Conexión entre equipos de borde PE y equipos de Core P	Tráfico Promedio Total de la Interfaz (Mbps)	Tramas Ethernet IPv4 (Frame x seg)	Tramas Ethernet IPv6 (Frame x seg)	Tráfico Total con IPv6 (Mbps)	Tráfico Promedio Adicional (Mbps)
MACHACHI PE - QUITOCENTRO P	365,1	30425,8	608516,7	370,0	4,9
ISLA TRINITARIA PE - GUAYAQUIL P	356,5	29708,3	594166,7	361,3	4,8
GUAYAQUIL KENEDDY PE - GUAYAQUIL P	571,7	47641,7	952833,3	579,3	7,6
CUENCA GUALACEO PE- CUENCA P	389,8	32483,3	649666,7	395,0	5,2
ESTACION TERRENA PE - QUITOCENTRO P	217,8	18150,0	363000,0	220,7	2,9
NUEVA LOJA PE - IÑAQUITO P	444,42	37035,0	740700,0	450,3	5,9
FRANCISO ORELLANA PE - IÑAQUITO P	545,7	45475,0	909500,0	553,0	7,3
DATA_CENTER PE - IÑAQUITO P	533,92	44493,3	889866,7	541,0	7,1
GUAYAQUIL_CENTRO PE- GUAYAQUIL_CENTRO P	219,06	18255,0	365100,0	222,0	2,9
GUAYAQUIL_CORREOS PE - GUAYAQUIL_CENTRO	121,5	10125,0	202500,0	123,1	1,6
GYS_BOYACA PE - GYS_CENTRO P	160,4	13366,7	267333,3	162,5	2,1
IBARRA_CENTRO1 PE - IBARRA_CENTRO P	2394,86	199571,7	3991433,3	2426,8	31,9
IBARRA_CENTRO2 PE - IBARRA_CENTRO P	339,18	28265,0	565300,0	343,7	4,5
FRANCISO_ORELLANA PE- PUYO P	326,5	27208,3	544166,7	330,9	4,4
TENA PE- PUYO P	249,66	20805,0	416100,0	253,0	3,3
NUEVA_LOJA PE- PUYO P	614	51166,7	1023333,3	622,2	8,2
BABAHOYO_QUEVEDO PE- MANTA P	438,6	36550,0	731000,0	444,4	5,8
SANTA_ELENA PE- MANTA P	291	24250,0	485000,0	294,9	3,9
Santo Domingo PE - SANTO DOMINGO P	5100	425000,0	8500000,0	5168,0	68,0
SAME PE - SANTO DOMINGO P	387,8	32316,7	646333,3	393,0	5,2
PORTOVIEJO PE - SANTO DOMINGO P	317	26416,7	528333,3	321,2	4,2

Tabla 10. Análisis de Trafico con IPv6 entre equipos PE-P. [Elaborado por el autor]

5.4 SIMULACIÓN SITUACIÓN ACTUAL DE LA RED IP/MPLS.

Con el objetivo de verificar los cambios que se deben realizar en la configuración de los equipos que componen la red IP/MPLS de CNT EP, se procede primeramente a simular la situación actual de la red, para lo que se utilizara la software GNS3. Para la simulación se empleara el diseño Jerárquico que contara con dos equipos core P, tres equipos de distribución o de borde PE que a su vez actuaran como equipos de acceso, para lo cual se utilizara el siguiente direccionamiento IP que se detalla en la Tabla 10.

EQUIPO	INTERFAZ	DIRECCION IP	MASCARA
UIOCNTP01	fa 0/0	10.6.0.1	255.255.255.252
	fa 1/1	10.2.1.1	255.255.255.252
	fa 1/0	10.2.2.1	255.255.255.252
	loop 100	172.30.10.20	255.255.255.255
AMBCNTP01	fa 0/0	10.6.1.0.2	255.255.255.252
	Fa 1/0	10.6.1.1	255.255.255.252
	loop 100	172.30.10.30	255.255.255.255
UIOCNTE01	fa 1/0	10.2.1.2	255.255.255.252
	loop 100	172.30.10.70	255.255.255.255
UIOMSCE01	fa 1/0	10.2.2.2	255.255.255.252
	loop 100	172.30.10.60	255.255.255.255
AMBCNTE01	fa 1/0	10.6.1.2	255.255.255.252
	loop 100	172.30.10.60	255.255.255.255

Tabla 11. Direccionamiento IP Simulación Actual de Red. [Elaborado por el autor]

EQUIPO	NET	Loop
UIOCNTP01	49.0001.1720.3001.0020.00	172.30.10.20
AMBCNTP01	49.0001.1720.3001.0030.00	172.30.10.30
UIOCNTE01	49.0001.1720.3001.0070.00	172.30.10.70
AMBCNTE01	49.0001.1720.3001.0040.00	172.30.10.40
UIOMSCE01	49.0001.1720.3001.0060.00	172.30.10.60

Tabla 12. Direccionamiento IP Para activar IS-IS. [Elaborado por el autor]

Con el direccionamiento IP citado se empleara el simulador GNS3 para configurar los equipos y parámetros como: interfaces físicas y lógicas, direcciones IPv4, protocolos

como ISIS, MPLS, BGP, VPNv4. La configuración de los protocolos se detalló en la apartado 5.1.3. En esta sección se verificara el funcionamiento de los protocolos y se realizara pruebas de conectividad entre los equipos que forman la red IP/MPLS y entre los equipos del cliente con la red del proveedor. En la figura 27 se presenta el esquema utilizado para la simulación.

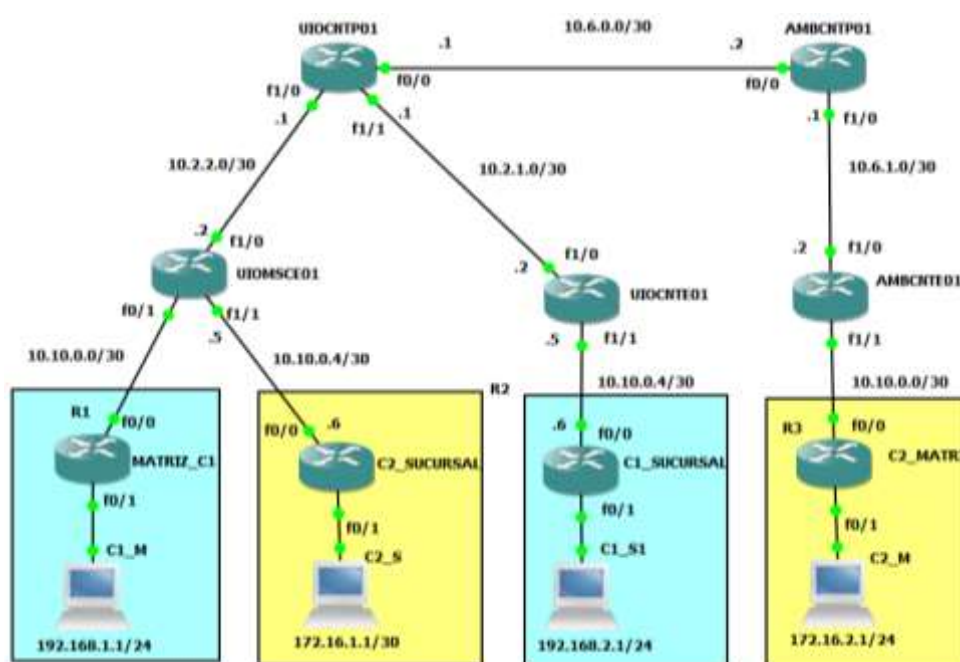


Figura 27. Esquema simulado de la Situación Actual de la Red IP/MPLS. [17]

Luego de realizar las configuraciones de las interfaces y habilitación de protocolos, se procede con las pruebas para verificar que los protocolos estén operativos y exista conectividad. En la figura 28 se revisa que el protocolo LDP esté habilitado en las interfaces utilizando el comando *show mpls interface*, complementariamente se verifica la generación tabla de reenvío de etiquetas que sirve para alcanzar a los diferentes equipos de la red MPLS indicando por cual interfaz se envía el paquete, para esto se utiliza el comando *show mpls forwarding-table*, en la figura 29 se examina el protocolo de enrutamiento interno IS-IS que esta funcionando y se genera una topología de la red.

```

UIOCNTP01#show mpls interfaces
Interface          IP          Tunnel  Operational
GigabitEthernet0/0 Yes (ldp)   No      Yes
FastEthernet1/0    Yes (ldp)   No      Yes
FastEthernet1/1    Yes (ldp)   No      Yes

UIOCNTP01#show mpls ldp discovery
Local LDP Identifier:
172.30.10.20:0
Discovery Sources:
Interfaces:
    GigabitEthernet0/0 (ldp): xmit/rcv
        LDP Id: 172.30.10.30:0
    FastEthernet1/0 (ldp): xmit/rcv
        LDP Id: 172.30.10.60:0
    FastEthernet1/1 (ldp): xmit/rcv
        LDP Id: 172.30.10.70:0

UIOCNTP01#show mpls forwarding-table
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
16 Pop tag 172.30.10.60/32 6231 Fa1/0 10.2.2.2
17 Pop tag 172.30.10.70/32 9379 Fa1/1 10.2.1.2
18 Pop tag 172.30.10.30/32 0 Gi0/0 10.6.0.2
19 17 172.30.10.40/32 0 Gi0/0 10.6.0.2
20 Pop tag 10.6.1.0/30 1848374 Gi0/0 10.6.0.2

```

Figura 28. Verificación de funcionamiento Protocolo MPLS. [17]

```

UIOCNTP01#show ip protocol
Routing Protocol is "isis"
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set

UIOCNTP01#show isis topology

IS-IS paths to level-2 routers
System Id      Metric  Next-Hop      Interface  SNPA
UIOCNTP01     --
AMBCNTE01     10      AMBCNTE01     Gi0/0      c=00.0528.0008
AMBCNTE01     20      AMBCNTE01     Gi0/0      c=00.0528.0008
UIOMSCE01     10      UIOMSCE01     Fa1/0      c208.2+24.0000
UIOCNTE01     10      UIOCNTE01     Fa1/1      c207.2+24.0000

UIOCNTP01#show isis neighbors

System Id      Type Interface IP Address  State Holdtime Circuit Id
AMBCNTE01     L2 Gi0/0     10.6.0.2   UP 2s 00
UIOCNTE01     L2 Fa1/1     10.2.1.2   UP 2s 00
UIOMSCE01     L2 Fa1/0     10.2.2.2   UP 2s 00

```

Figura 29. Verificación de funcionamiento Protocolo ISIS. [17]

```

UIOMSCE01#show bgp all
For address family: IPv4 Unicast

For address family: IPv6 Unicast

For address family: VRFv4 Unicast
BGP table version is 0, local router ID is 172.30.10.60
Status codes: s - suppressed, d - dampened, h - history, * - valid, > best, i - internal,
               x - RIB-failure, S - Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 20006410 (default for vrf E1)
*> 0.0.0.0           10.10.0.2           0         32768 ?
*> 10.10.0.0/30       0.0.0.0             0         32768 ?
*>10.10.0.4/30        172.30.10.70        0 100      0 ?
*>10.10.0.2.0         172.30.10.70        0 100      0 ?

```

Figura 30. Verificación de funcionamiento Protocolo BGP. [17]

En la figura 31 se realiza pruebas de conectividad utilizando el comando ping en los equipos de UIOMSCE01 y AMBCNTE01 verificando que la conectividad se ha establecido correctamente, el comando traceroute indica la ruta IP que se sigue el paquete para alcanzar a

los otros equipos. Con la configuración básica de los protocolos IS-IS, MPLS, BGP, direcciones IPv4 se ha establecido conectividad entre los equipos que forman la red IP/MPLS del proveedor.

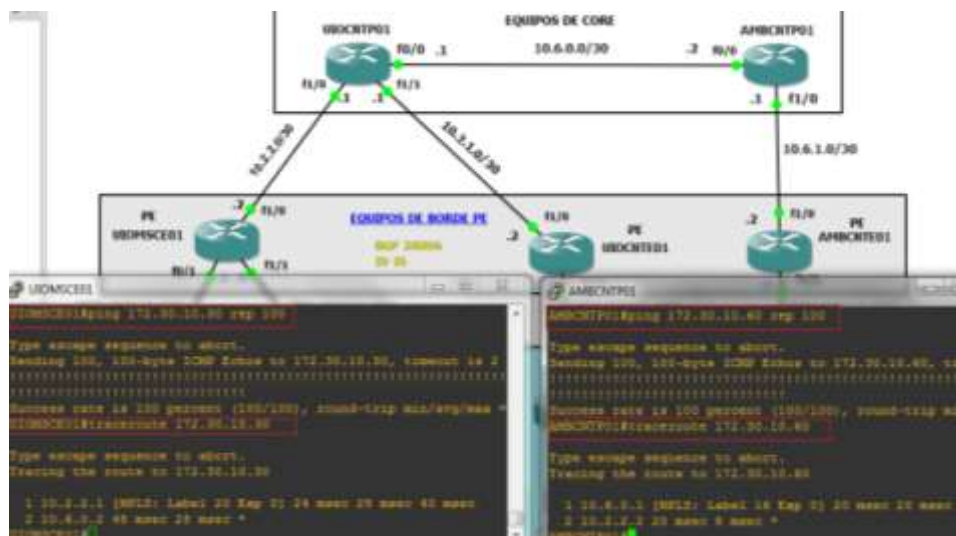


Figura 31. Prueba de conectividad desde UIOMSCE01 a AMBCNTE01. [17]

Complementariamente se simula la configuración de clientes corporativos con servicio de datos en el cual se utiliza instancias de enrutamiento VRF para segmentar los servicios. En la Tabla 13 se detalla el direccionamiento IPv4 y VRF utilizado para establecer conectividad entre el equipo del cliente CE y la red del proveedor. En la figura 32 se realiza pruebas de conexión entre las redes del cliente, para este ejemplo la matriz se encuentra configurada en UIOMSCE01 y la sucursal UIOCNTE01, pudiendo observar que se tiene resultados positivos.

	WAN_CLIENTE	IP_LAN	VRF
Cliente_1_Matriz_Mariscal	10.10.0.2/30	192.168.1.1/24	C1
Cliente_1_Matriz_Centro	10.10.0.6/30	192.168.2.1/24	C1
Cliente_2_Matriz_Mariscal	10.10.0.0/30	172.16.2.0/24	C2
Cliente_2_Sucursal_Ambato	10.10.0.4/30	172.16.1.0/24	C2

Tabla 13. Direccionamiento IP para Cliente corporativo. [Elaborado por el autor]

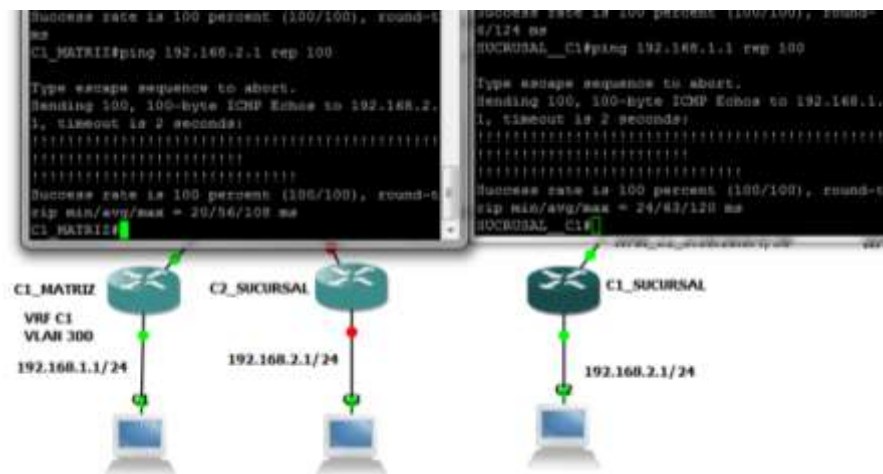


Figura 32. Pruebas de conectividad de clientes. [17]

Una vez simulado la configuración de la red actual y realizada las pruebas de conectividad con clientes finales, se procederá a validar los cambios en las configuraciones de la red para poder implementar el método 6VPE.

5.5 SIMULACIÓN DE RED IP/MPLS IMPLEMENTADO IPV6 CON EL MÉTODO 6VPE

Con el objetivo de minimizar los errores de configuración en la red activa se procederá a simular el método 6VPE el cual fue recomendado en los ítems anteriores. En esta sección se centrará básicamente en las configuraciones de direccionamiento IPv6, habilitación de protocolos como VPNv6, VRF, y pruebas de conectividad. Los cambios lógicos que se realiza son en los equipos de borde PE y el equipo del cliente CE ya que el core no existe modificaciones lo cual se comprobara en las pruebas que se realizará.

Diagrama red IP/MPLS con el Método 6VPE para habilitar IPv6.

Como se indicó el método 6VPE no requiere modificación los equipos de core, los cambios en la configuración se realiza en los equipos de borde PE, en donde se habilitara las interfaces y protocolos que se detallan en la presente sección. La figura 33 se visualiza el diagrama y direccionamiento IP utilizado para simulación con el método 6VPE, adicional se distingue que el core de MPLS mantiene el direccionamiento IPv4 (el mismo que la situación actual) de igual manera se conserva la configuración del protocolo Interno IS-IS y del protocolo BGP.

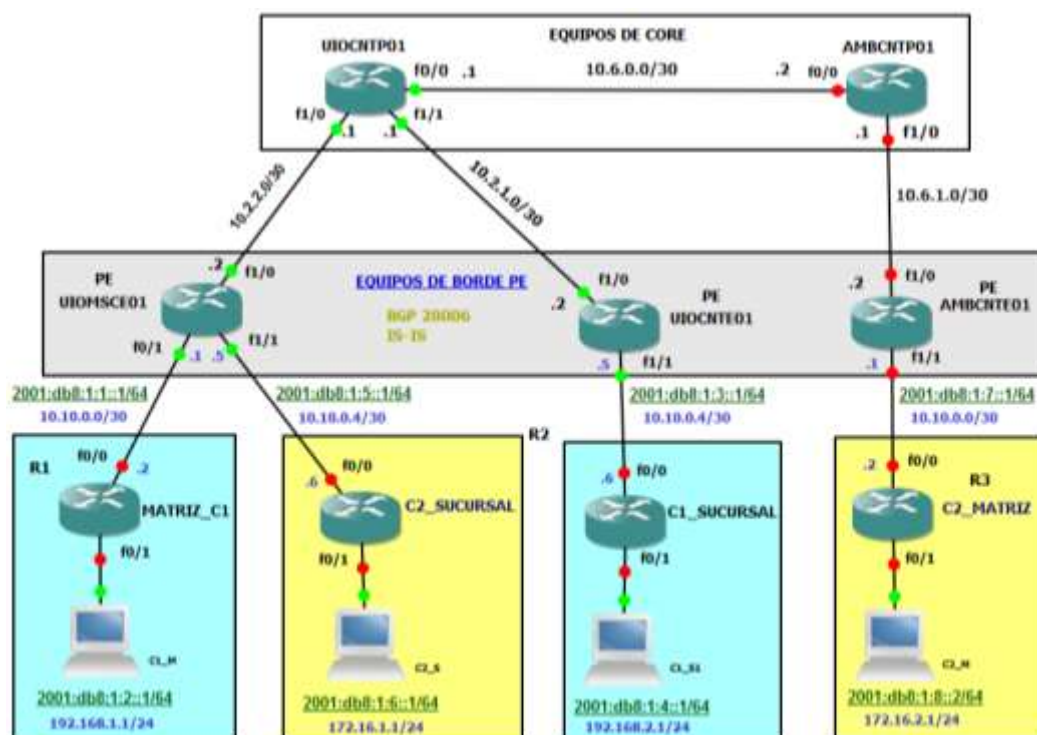


Figura 33. Esquema y direccionamiento IP para simulación del método 6VPE. [17]

Habilitación del protocolo de internet IPv6

Los equipos de Core CNT EP y los de de borde PE son de marca Cisco, para habilitar el protocolo IPv6 , el routing y reenvío de paquetes se ingresan los siguientes comandos.

```
UIOMSCE01(config)# ipv6 unicast-routing
UIOMSCE01(config)# ipv6 cef
```

Configuración Instancia de enrutamiento VRF para cliente

Al igual que en la configuración actual de la red, se crea VRF para tener múltiples instancias de enrutamiento de modo simultaneo en un router. En este caso la configuración varia levemente ya que se utiliza el comando **VRF definition** el cual soporta múltiples protocolos y se puede habilitar IPv4 e IPv6 dentro de la misma VRF. Con el método 6VPE seleccionado permite crear VPN en MPLS y segmentar los servicios de los clientes. En la figura 34 se detalla los comandos utilizados para configurar VRF definition, donde se puede observar que los comandos para IPv6 e IPv4 son los mismos y se mantiene el esquema de la red actual.

```

vrf definition C1_6VPE
 rd 28006:70
 !
 address-family ipv4
  route-target export 28006:70
  route-target import 28006:70
 exit-address-family
 !
 address-family ipv6
  route-target export 28006:70
  route-target import 28006:70
 exit-address-family

```

Figura 34. Configuración de VRF definition. [17]

Configuración dirección IPv6 en la interfaz

Para configurar el direccionamiento IPv6 se lo puede realizar en una interfaz virtual mediante el uso de Vlan's o en una interfaz física y asociar la VRF que se creó previamente, para este ejemplo se configuró en una interfaz física la dirección IPv6, cabe recordar que se indicó que los equipos PE son Dual Stack por lo que se configura las dos pilas de protocolos sobre la misma interfaz. En la Tabla 14 se detalla el direccionamiento IPv6 para establecer conectividad desde la red IP/MPLS hacia la red del cliente, lo cual se configura en los equipos de borde PE.

	WAN_MPLS_CLIENTE	IP_LAN	VRF
Cliente 1 Matriz	2001:db8:1:1::1/64	2001:db8:1:2::1/64	C1_6VPE
Cliente 1 Sucursal	2001:db8:1:3::1/64	2001:db8:1:4::1/64	C1_6VPE
Cliente 2 Matriz	2001:db8:1:5::1/64	2001:db8:1:6::2/64	C2_6VPE
Cliente 2 Sucursal	2001:db8:1:7::1/64	2001:db8:1:8::2/64	C2_6VPE

Tabla 14. Direccionamiento IPv6 utilizado para simulación. [Elaborado por el autor]

En la figura 35 se adjunta los comandos para habilitar IPv6 en equipo PE y asociarlo con la instancia de enrutamiento VRF, adicional se puede notar que sobre la misma interfaz se encuentra habilitado IPv4 e IPv6.

```

UIOMSCE01#sh run int fa 0/1
Building configuration...

Current configuration : 200 bytes
!
interface FastEthernet0/1
description WAN_C1_MATRIZ
vrf forwarding C1_6VPE
ip address 10.10.0.1 255.255.255.252
duplex full
speed 100
ipv6 address 2001:DB8:1:1::1/64
ipv6 nd ra suppress
end

```

Figura 35. Configuración interfaz con IPv6. [17]

Configuración Red Privada Virtual (VPNv6) en MPLS

Al mantener la configuración de los protocolos IS-IS, MPLS y BGP, se puede levantar red privada o VPN versión 6 el cual se establece las vecindades con otros equipos de borde donde la VPN tenga presencia y permite identificar unívocamente a un cliente. Esta configuración se lo realiza dentro del proceso BGP 28006. En la figura 36 se puede observar que mantiene la configuración de la red actual del protocolo BGP, pero dentro del address-family se añade un VPNv6.

```

!
address-family vpnv6
neighbor 172.30.10.70 activate
neighbor 172.30.10.70 send-community both
exit-address-family
!
address-family vpnv4
neighbor 172.30.10.40 activate
neighbor 172.30.10.40 send-community both
neighbor 172.30.10.70 activate
neighbor 172.30.10.70 send-community both
exit-address-family
!

```

Figura 36. Configuración VPNv6. [17]

La configuración para poder distribuir las rutas que se aprende entre el equipo del cliente CE y el equipo de borde PE es muy similar a la configuración de la red actual, en esta sección se indica que se utiliza el protocolo IPv6 y se distribuye estáticamente las rutas. En la figura 37 se puede observar que los comandos para redistribuir rutas en IPv6 es la misma que utiliza para IPv4, pero en diferentes address-family y utilizando la misma instancia de enrutamiento VRF.

```

address-family ipv4 vrf C1_6VPE
 redistribute connected
 redistribute static
 default-information originate
 no synchronization
 exit-address-family
!
address-family ipv6 vrf C1_6VPE
 redistribute connected
 redistribute static
 default-information originate
 no synchronization
 exit-address-family
!

```

Figura 37. Configuración address-family IPv6. [17]

5.5.1 Configuración IPv6 en el equipo el cliente CE

Otro punto que se debe tomar en consideración al utilizar 6VPE es que el equipo del cliente debe ser Dual Stack, en este caso para entregar servicios corporativos la CNT EP utiliza equipos de marca Cisco de la serie 800 – 1940 - 2600 que cumplen con esta característica, pudiendo de esta manera habilitar el protocolo IPv4 e IPv6 de manera simultánea. En la tabla 15 se detalla el direccionamiento IPv6 que se utilizara para poder establecer conectividad entre el cliente y el Backbone de CNT EP. En la figura 38 se observa la configuración de la interfaz que sirve de conexión con entre el cliente y la Red IP/MPLS

	WAN_CLIENTE	IP_LAN
Cliente_1_Matriz_Mariscal	2001:db8:1::2/64	2001:db8:2::1/64
Cliente_1_Matriz_Centro	2001:db8:3::1/64	2001:db8:4::1/64
Cliente_2_Sucursal_Mariscal	2001:db8:5::2/64	2001:db8:6::1/64
Cliente_2_Matriz_Ambato	2001:db8:7::1/64	2001:db8:8::1/64

Tabla 15. Direccionamiento IPv6 configurado en el cliente. [Elaborado por el autor]



Figura 38. Configuración IP_WAN cliente. [17]

5.5.2 Comparación de configuración de IPv4/ IPv6 sobre red IP/MPLS utilizando el método 6VPE.

En la Tabla 16 se realiza un resumen de las configuraciones que se tiene actualmente con IPv4 y los cambios que se debe realizar para poder habilitar el método de tunel 6VPE que fue recomendado para la migración y coexistencia de IPv4 & IPv6. Como se puede observar las diferencias son mínimas, específicamente en los equipos de borde PE se debe configurar las direcciones IPv6 en las interfaces, dentro del proceso BGP se habilitar VPNv6 donde tenga presencia la VRF del cliente, para que las instancias de enrutamiento VRF soporte los dos protocolos IPv4 / IPv6 simultáneamente, se habilita VRF definition. Básicamente seria los cambios que se deben aplicar en los equipos de borde PE dentro de la red del proveedor para poder establecer el método 6VPE.

Protocolo		IPv4	IPv6 (método 6VPE)	Observaciones
CEF		<i>Router(config)#ip cef</i>	<i>Router(config)#ipv6 cef</i>	
		<i>Router(config)#ip routing</i>	<i>Router(config)#ipv6 unicast-routing</i>	habilitación de routing en los equipos
MPLS	Interfaz loopback	<i>Router(config)#interface loopback 100</i>	<i>Router(config)#interface loopback 100</i>	
	Router ID	<i>mpls ldp router-id Loopback100</i>	<i>mpls ldp router-id Loopback100</i>	
	MPLS	<i>Router(config)#mpls ip</i>	<i>Router(config)#mpls ip</i>	Habilitar protocolo MPLS
	LDP	<i>Router(config-if)#mpls label protocol ldp</i>	<i>Router(config-if)#mpls label protocol ldp</i>	Habilitar protocolo de distribución de etiquetas en las interfaces
Protocolo IGP	IS-IS	<i>Router(config)#ip router isis</i>	<i>Router(config)#ip router isis</i>	
	IS-IS en la interfaz	<i>Router(config-if)#ip router isis</i>	<i>Router(config-if)#ip router isis</i>	
		<i>Router(config-if)#isis network point-to-point</i>	<i>Router(config-if)#isis network point-to-point</i>	
BGP	BGP	<i>Router(config)#router bgp 28006</i> <i>Router(config)#bgp router-id</i>	<i>Router(config)#router bgp 28006</i> <i>Router(config)#bgp router-id</i>	
	Address Family VPNvX	<i>Router(config-router)#address-family vpnv4</i>	<i>Router(config-router)#address-family vpnv6</i>	Se configura el túnel, se establece los peer BGP.
	Address Family IPvX	<i>Router(config-router)#address-family ipv4 vrf</i>	<i>Router(config-router)#address-family ipv6 vrf nombre vrf</i>	
Estancia de enrutamiento	VRF	<i>Router(config)#ip vrf C1</i> <i>rd 28006:10</i> <i>route-target export 28006:10</i> <i>route-target import 28006:10</i>	<i>Router(config)#vrf definition</i> <i>rd 28006:70</i> <i>address-family ipv6</i> <i>route-target export 28006:70</i> <i>route-target import 28006:70</i> <i>exit-address-family</i>	En IPv6 se crea vrf definition permite configurar IPv4 e IPv6
Dirección IP	Interfaz	<i>Router(config-if)#ip address IPv4_address msk</i>	<i>Router(config-if)#ipv6 address ipv6-address/prefix-length / prefix-name sub-bits/prefix-length</i>	

Tabla 16. Comparación de Configuración IPv4 y el método 6VPE. [Elaborado por el autor]

5.5.3 Resultados al implementar 6VPE en la red IP/MPLS

Verificar VPNv6-MPLS en los equipos de borde donde la VRF tenga presencia.

Se verifica la MPLS-VPNv6 que se establecido a través del protocolo BGP el cual mantiene la misma configuración tanto para VPN en IPv4 e IPv6 pero en diferentes address-family . En la figura 39 se observa la VPNv6 del cliente 1 que utiliza la VRF *CI_6VPE* desde el equipo de UIOMSCE01 hacia UIOCNTE01 (router id 172.30.10.70), el cual esta está aprendido las redes IPv6 configuradas en el equipo de borde UIOCNTE01. Se demuestra que las configuraciones en los equipos de Core se mantienen y no se modifican.

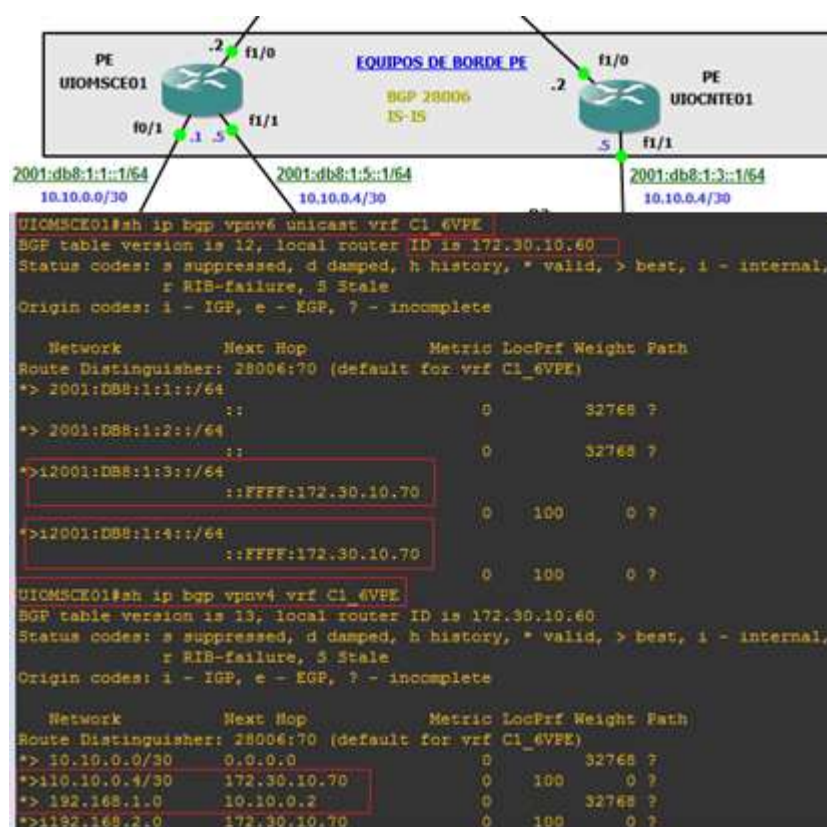
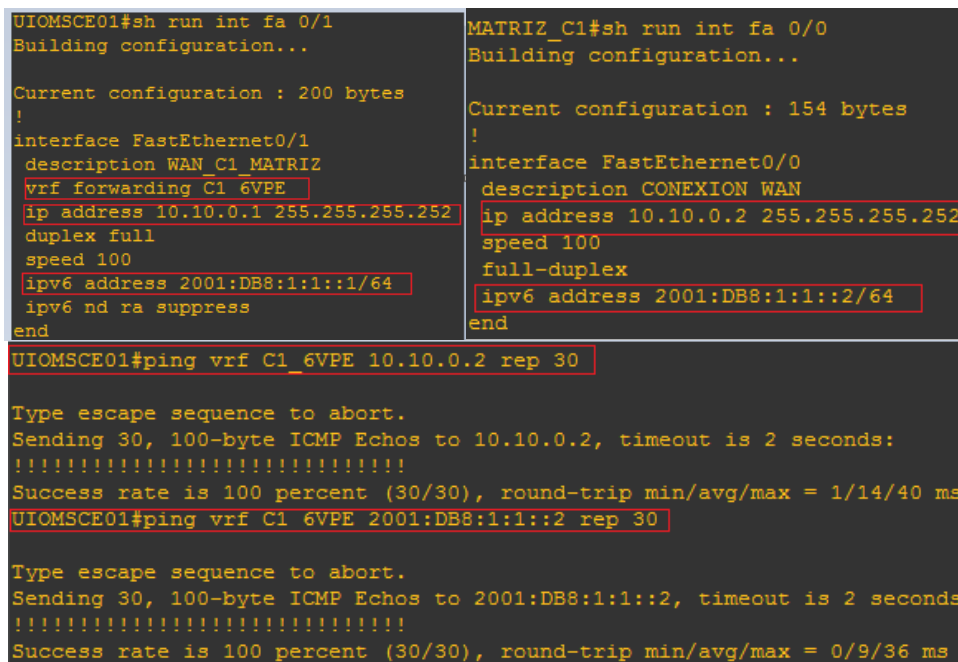


Figura 39. Verificación del Tunel VPNv6 –MPLS cliente 1. [17]

Coexistencia de Protocolo IPv4 e IPv6 en los equipos de borde PE

En el método 6VPE uno de los requisitos es que los equipo de borde PE y el equipo CE deben ser Dual Stack, lo cual se indicó anteriormente que los dispositivos que utilizan

CNT EP soporta esta característica, adicionalmente se simulo la configuración para establecer conectividad IPv4 e IPv6 sobre la misma interfaz y utilizando la misma VRF. En la figura 40 se puede observar que se habilito los dos protocolos en los equipos PE y CE y se realizó pruebas de conectividad siendo estas exitosas.



```

UIOMSCE01#sh run int fa 0/1
Building configuration...

Current configuration : 200 bytes
!
interface FastEthernet0/1
 description WAN C1 MATRIZ
 vrf forwarding C1_6VPE
 ip address 10.10.0.1 255.255.255.252
 duplex full
 speed 100
 ipv6 address 2001:DB8:1:1::1/64
 ipv6 nd ra suppress
end

MATRIZ_C1#sh run int fa 0/0
Building configuration...

Current configuration : 154 bytes
!
interface FastEthernet0/0
 description CONEXION WAN
 ip address 10.10.0.2 255.255.255.252
 speed 100
 full-duplex
 ipv6 address 2001:DB8:1:1::2/64
end

UIOMSCE01#ping vrf C1_6VPE 10.10.0.2 rep 30

Type escape sequence to abort.
Sending 30, 100-byte ICMP Echos to 10.10.0.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (30/30), round-trip min/avg/max = 1/14/40 ms
UIOMSCE01#ping vrf C1_6VPE 2001:DB8:1:1::2 rep 30

Type escape sequence to abort.
Sending 30, 100-byte ICMP Echos to 2001:DB8:1:1::2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (30/30), round-trip min/avg/max = 0/9/36 ms

```

Figura 40. Pruebas de conectividad IPv4 e IPv6 del cliente utilizando VRF. [17]

Conectividad desde los equipos de Borde PE a la Instancia de Enrutamientos VRF de los clientes.

Luego de habilitar las interfaces, habilitar los protocolos para el método 6VPE se procede verificar que exista conectividad con IPv6, en la figura 41 se realizan pruebas de conectividad IPv6 desde los equipos de borde PE UIOMSCE01 Y UIOCNTE01 en donde la VRF C1_6VPE del Cliente_1 tiene presencia, al utilizar el comando ping se valida la conectividad. En la figura 42 se verifica de conectividad desde los equipos del cliente CE de Matriz y Sucursal_1, los cuales deben pasara por los equipos de borde y de core de la red del proveedor.

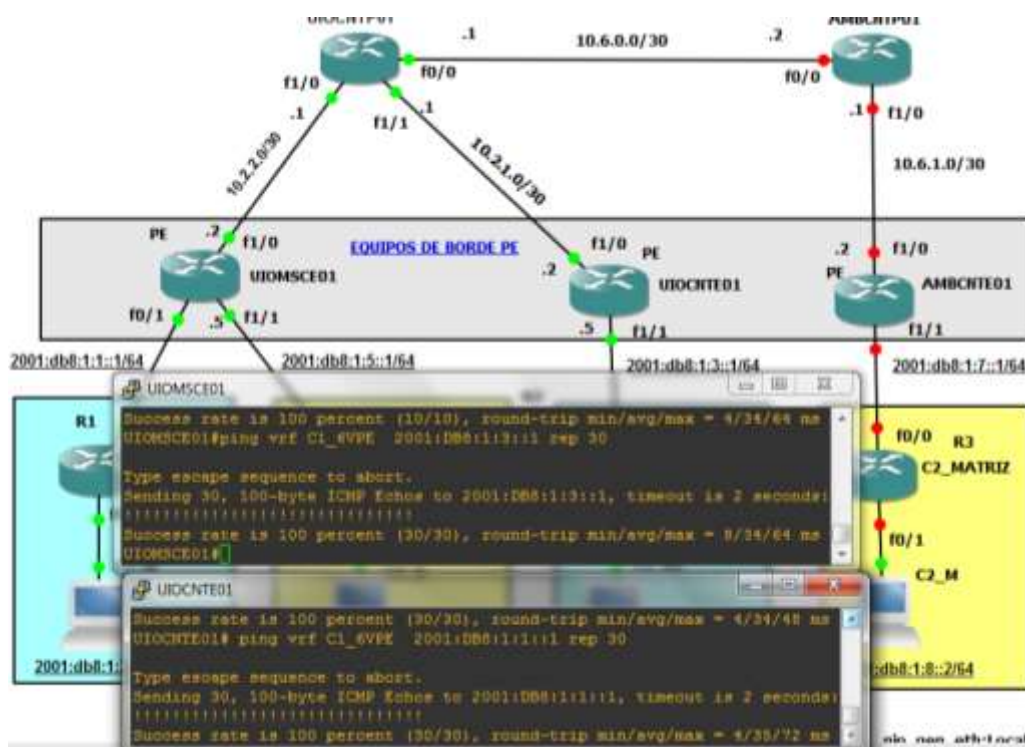


Figura 41. Pruebas de conectividad desde MPLS hacia la WAN. [17]

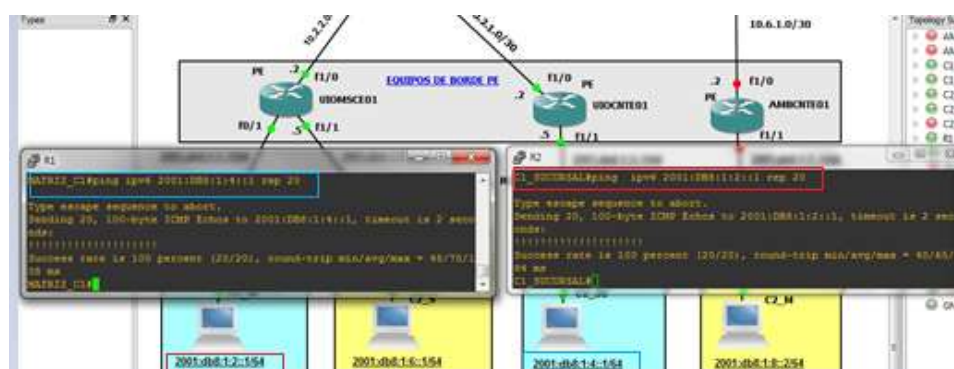


Figura 42. Pruebas de conectividad equipos CE de Matriz y Sucursal del Cliente_1. [17]

Verificación que los equipos de Core mantienen direccionamiento IPv4

En la Figura 43 se realiza una traza con dirección IPv6 desde CE_Matriz hacia el CE_Sucursal del Cliente 1, en donde se observa que cuando entra a la red IP/MPLS utiliza la conexión UIOMSCE01 Y UIOCNTE01 que está configurado con IPv4 (10.2.2.1) es decir el paquete IPv6 es enviado utilizando la infraestructura IPv4 con la que funciona actualmente la Red MPLS de CNT, verificando de esta forma que el core no se ve afectado en la configuración.

```
MATRIZ_CI#tracert 2001:DB8:1:4::1
Type escape sequence to abort.
Tracing the route to 2001:DB8:1:4::1
 0  2001:DB8:1:1::1  4 msec 16 msec 8 msec
 1  ::FFFF:10.2.2.1  32 msec 68 msec 48 msec
 2  2001:DB8:1:3::1  60 msec 56 msec 52 msec
 3  2001:DB8:1:4::1  40 msec 88 msec 72 msec
MATRIZ_CI#
```

Figura 43. Prueba tracer desde CPE_Matriz hacia CPE_sucursal. [17]

5.6 ANÁLISIS DE LA MIGRACIÓN & COEXISTENCIA DE IPV4 E IPV6 PARA CLIENTES CORPORATIVOS EN LA RED IP/MPLS DE CNT EP

Cabe señalar que el método recomendado es 6VPE para poder establecer conectividad a clientes corporativos con el nuevo protocolo IPv6 y analizar los cambios que se deben realizar en la backbone de la Red MPLS. Entre las ventajas de la técnica de migración y coexistencia se puede citar:

- El aumento de direcciones IP disponibles.
- Coexistencia con IPv4, que hará posible una migración paulatina al nuevo protocolo de internet IPv6 ya que el método es escalable.
- No se necesita actualización de Hardware y software en el backbone de la Red
- Las configuraciones lógicas de IPv4 & IPv6 en la red son muy similares, básicamente se modifican los protocolos e interfaces que sirven para conectar a los clientes tanto en el equipo de borde PE y en el equipo del cliente CE.
- La situación actual de Red MPLS de CNT EP facilita la migración al método 6VPE ya que no se necesita realizar modificaciones en el Core.
- Al utilizar un método de tunnelling, el aumento de tráfico con IPv6 es mínimo

Al establecer el nuevo método también existen desventajas que entre las que se puede citar:

- Se necesita capacitar personal para poder brindar soporte adecuado a los clientes.
- El método 6VPE indicado en el presente trabajo es para entregar servicios de conectividad a clientes corporativos con configuraciones estándar, en caso de existir requerimientos especiales se tendrá que validar si el método cumple con las características solicitadas.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- El Principal problema en la migración / coexistencia es la incompatibilidad de los protocolo IPv4 e IPv6.
- La características de red y configuraciones que dispone CNT-EP actualmente, facilita la migración / coexistencia de IPv4 & IPv6, ya que se utiliza VRF, MPLS BGP y protocolo IS-IS que tiene la particularidad de soportar múltiples protocolos capa 3.
- El método general de migración utilizado es “Tunneling ”, donde se analizó los diferentes métodos de **IPv6 sobre MPLS** determinando que 6VPE es el que más se ajusta a las necesidades actuales de CNT EP ya que permite mantener la configuración en los equipos de Core y realizar leves modificaciones en los equipos de borde PE y en los equipos del cliente CE.
- Los equipos de borde PE que forman parte de la Red IP/MPLS no necesitan modificaciones a nivel de hardware y software por lo que soporta la configuración para el método de migración 6VPE
- Al utilizar método de tunneling, el aumento de Tráfico con el protocolo IPv6 es mínimo en las interfaces de interconexión entre los equipos de borde PE y los equipos de Core P.
- Los cambios en la configuración de la Red IP/MPLS de CNT EP para implementar el método 6VPE son mínimos, se configura direccionamiento IPv6, en el proceso BGP se configura familia de direcciones IPv6 y el método de distribución de rutas.
- IPv6 sobre MPLs no es un método para solucionar el problema de agotamiento de IPv4 la solución es cuando se utilice IPv6 nativo

6.2 Recomendaciones

- Se recomienda que se utilice un método de transición a IPv6 y no migrar la Red MPLS a IPv6 nativo, ya que este proceso será progresivo en tiempo y en costo.
- Se recomienda configurar IPv6 e IPv4 en una sola interfaz lógica o física en la Red del proveedor para poder brindar el servicio al cliente final.
- En caso que el cliente disponga de su propio equipo CE se debe verificar que soporte Dual Stack para que pueda funcionar con el método propuesto.
- Se recomienda establecer un método de asignación de IPv6 a clientes finales es decir cuál sería prefijo de red a utilizarse para WAN y LAN.

7. BIBLIOGRAFIA

Libros

- [1] **Acosta A. , Aggio S.,& Cicileo G. ,& Lynch T. ,& Moreiras A. ,& Rocha M., & Servin A. & Berenguer S.** (2014). *IPv6 para Operadores de Red*. Buenos Aires Argentina
- [2] **Morrone L.** (2011). *Mecanismos de Transición hacia redes IPv6* (Tesis de Especialista). Universidad Nacional de la Plata. Argentina
- [3] **Evans J., & Filsfils C.** (2007) *Deploying IP and MPLS QoS For Multiservice Network*. San Francisco EE.UU: Morgan Kaufmann Publishers
- [4] **Cisco System, Inc.** (2012) *IPv6 Configuration guide, Cisco IOS Release 15.2MT*. San Jose California – EE.UU.
- [5] **Arroyo J.** (2014). *Adecuación de Red de ISP para soporte IPv6*. Universidad Nacional Autónoma de México. México
- [6] **Clercq J. , Ooms D. , Prevost S.** *Connecting “IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)”* . RFC 4798, Febrero 2007
- [7] **Clercq J. , Ooms D. , Prevost S.** *Connecting “ BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN* . RFC 4659, Septiembre 2006

Documentos Electrónicos

- [8] **Dávila E.** (2016). IPv6 en Redes MPLS (6PE, 6VPE y LDPv6). Recuperado 01 Mayo del 2016. De:

https://supportforums.cisco.com/sites/default/files/attachments/document/files/ipv6_en_redes_mpls_6pe_6vpe_y_ldpv6_version_final.pdf

[9] **Aizprúa J.** (2015). En Comparación 6PE y 6vPE. Recuperado 8 Febrero 2016. De <http://documents.mx/documts/comparacion-6pe-y-6vpe.html>

[10] **Auben.** (2014). BGP/MPLS Layer 3 VPN. Recuperado 9 Febrero 2016. De <http://www.auben.net/index.php/tecnologias/g-mpls-e-ingenieria-de-trafico/bgp-mpls-layer-3-vpn>

[11] **Cobos D.** (2014). MPLS VPNv6/VPNv4 sobre la red de transporte IPv4. Recuperado 9 Febrero 2016. De http://diariodeingenieria.blogspot.com/2014_04_01_archive.html.

[12] **Cisco System, Inc.** Implementig IPv6 over MPLS. Recuperado 2 Febrero 2016. De: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-over-mpls.html>

[13] **Outlander Founder.** CCNA V5 Español (200-120). Recuperado 5 Febrero 2016. De <http://ccna-v5.net/2015/05/ccna-v5-0-2015-online-curriculum.html>.

[14] **Cisco System, Inc.** Per-VRF Assignmennt of BGP Router ID. Recuperado 20 Febrero 2016. De http://www.cisco.com/c/en/us/td/docs/ios/12_2sr/12_2sra/feature/guide/srbgprid.html

[15] **Cisco System, Inc.** Cisco Networking Academy. Recuperado 5 Febrero 2016. De http://www.cisco.edu.mn/CCNA_R&S_1_%28Intruduction%20To%20Networking%29/

[16] **Akshay S.** (2014). MPLS VPN. Recuperado el 11 Febrero 2016 De : <http://ipmpls.com/mpls/mpls-write-up/>

Herramientas Sotware

[17] **Grossmann J, Duponchelle J.** (2015). GNS3 . version 1.4.6. GNS3 Technologies.

[18] **The Cacti Group.** (2015). Cacti. Version 0.8.8. The Cacti Group.

[19] **Cisco IOS Technologies.** (2012). Cisco Ios. Version 15.2 . Cisco system.